2 Linux optimal installieren und pflegen

OpenSUSE liefert wie alle erfolgreichen Linux-Distributionen sehr umfangreiche Dateiarchive und bietet eine sehr bequeme Installation.

Standardinstallationen können allerdings nicht alle denkbaren Einsatzfälle – vom Desktop-PC bis zum File- oder Webserver – vorhersehen und jede erdenkliche Hardware berücksichtigen.

Die Informationen dieses Kapitels sollen Ihnen vor, während und nach der Installation helfen, einen genau auf Ihre Bedürfnisse angepassten Linux-Server einzurichten:

- Hardware: Treiberverfügbarkeit prüfen vor dem Kauf (Kapitel 2.1). Dieser Abschnitt gibt Tipps, wie Sie vor dem Beschaffen von Hardware herausfinden, ob es für diese aktuelle Linux-Treiber gibt.
- Linux für Serverdienste planen (Kapitel 2.2): Linux-Server können kleinen und großen Netzen vielfältige Dienste anbieten. Während in kleinen Netzen vielleicht ein einfacher Ein-Prozessor-Server für alle Serverdienste ausreicht, wird man in größeren Netzen für jeden Dienst oder für Gruppen von Diensten getrennte oder gar redundante Linux-Server, vielleicht auch mit mehreren Prozessoren, benötigen. Dieser Abschnitt gibt Installationstipps für solche Fälle.
- Aufteilung der Festplatten planen und Partitionen einrichten (Kapitel 2.3).
- Linux für Serverdienste installieren (Kapitel 2.4) geht auf Strategien ein, schlanke Server einzurichten.
- Nachinstallieren von Paketen (Kapitel 2.5) zeigt Wege, für den Einsatzzweck notwendige Pakete von Quellen wie einer DVD oder aus dem Netz nachzuinstallieren.
- Adressen dynamisch verteilen (Kapitel 2.6): Statt jedem Gerät im Netz seine IP-Adresse per Hand zuzuweisen, kann man sie per Adressserver dynamisch verteilen. Der Abschnitt zeigt, wie Sie einen Server für das Dynamic Host Control Protocol (DHCP) einrichten.
- Postdienste konfigurieren (Kapitel 2.7): OpenSUSE hat eine Konfigurationsdatei vorbereitet, die auf Ihre Angaben wartet.
- Informationen über Sicherheitsprobleme (Kapitel 2.8): Beachten Sie beim Installieren von Servern verantwortungsvoll die aus heutiger Sicht erkennbaren Sicherheits-

risiken und entwickeln Sie flexible Strategien, diesen Risiken während der gesamten Betriebszeit der Server jeweils aktiv zu begegnen.

- Nur ein aktuelles System kann sicher sein. Lesen Sie daher dringen, wie Sie Programme und Systemdateien aktualisieren (Kapitel 2.9).
- Einbruchserkennung und Virenschutz (Kapitel 2.10),
- Sichern der Stromversorgung mit einer USV (Kapitel 2.11),
- Datensicherung auf Bandlaufwerken, die höhere Kapazitäten besitzen als DVD-Laufwerke (Kapitel 2.12).

2.1 Hardware: Treiberverfügbarkeit prüfen vor dem Kauf

Prüfen Sie bitte vor dem Kauf von Hardware in Hardware-Datenbanken (z. B. `http://de.opensuse.org/Hardware_Kompatibilitätsliste`), ob

- die jeweiligen Hardware-Hersteller oder
- freie Linux-Entwickler

Linux-Treiber für diese Hardware erstellt haben.

Weigern sich Hersteller, zum Programmieren erforderliche technische Spezifikationen zu veröffentlichen oder halten sie Standards nicht ein, um Bauteile zu sparen, können Sie deren Hardware mit Linux nicht betreiben. Sparen Sie sich die Enttäuschung, für solche Geräte Geld auszugeben, da Sie hierfür keine Treiber für Linux finden können.

Bei Linux-Servern, die nicht unbedingt auf eine grafische Benutzeroberfläche angewiesen sind, sind die Netzwerkkarte und die ISDN-Karte kritisch, gelegentlich auch Festplatten-Controller (siehe 2.3.3). Bei Netzwerkkarten mit ganz neuen Chipsätzen kann es einige Wochen dauern, bis die aktuellen Linux-Distributionen ausgereifte Treiber enthalten. Preisgünstige Standardkarten mit den Chipsätzen von Realtek und Intel unterstützt Linux aber schon lange, natürlich auch für Gigabit-Ethernet.

In Regionen ohne DSL-Anbindung sind viele Anwender noch auf ISDN angewiesen. Statt mit alten ISA-Karten Zeit zu verlieren, sollten Sie lieber weit verbreitete PCI-Karten wie die Fritz!Card PCI von AVM verwenden.

2.2 Linux-Server planen

In heterogenen Netzarchitekturen größerer Firmen und Organisationen kommen auf einzelne Linux-Server andere Aufgaben zu als auf den einzigen Linux-Server in einem kleinen Netz für wenige Anwender.

Schon sehr früh vor dem Installieren sollte man planen, welche Aufgaben der jeweilige Server übernehmen soll.

Die Server für Anwendungen und jene für die Datenspeicherung sollte man komplett voneinander trennen. Soll ein Server sowohl Anwendungen ausführen als auch Benutzerdaten speichern, sollte man für statische Anwendungen und dynamische Daten zumindest getrennte Laufwerkssysteme oder getrennte Partitionen einrichten. So lässt sich verhindern, dass Benutzer die Root-Partition der Festplatte überschwemmen und damit das ganze System blockieren. Außerdem ist es so leichter, für Anwendungen und Daten verschiedene Sicherungsstrategien anzuwenden.

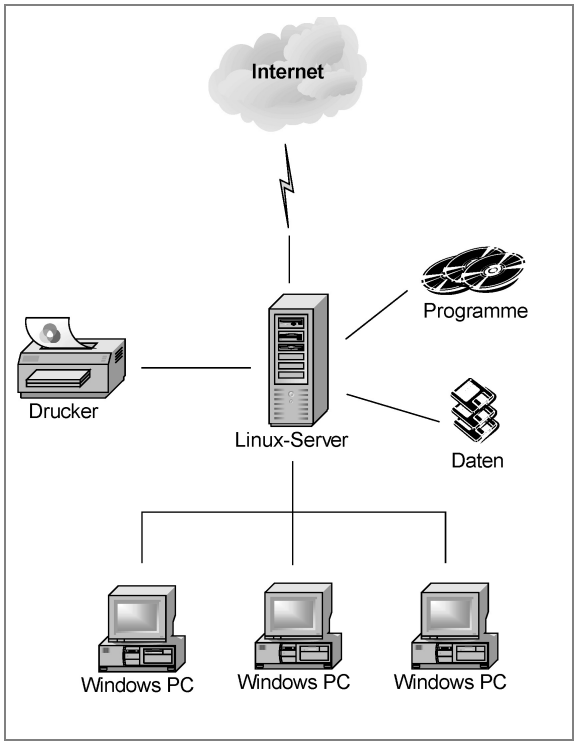

Abbildung 2.1: Linux-Einzelserver

Während der Plattenbedarf für Anwendungen leichter vorhersehbar ist, sollte man den Speicherplatz pro User durch sogenannte *Disk-Quotas* begrenzen (siehe Kapitel 3.3).

Die nächste Ausbaustufe könnte

- den Übergang vom Intranet zum Internet,
- das Speichern von Benutzerdaten und
- Anwendungen wie Internet- und Intranetdienste

auf drei Servern verteilen (Abbildung 2.2).

Bei diesen Konfigurationen braucht man nur die Datenträger der Datei-Server täglich zu sichern. Auch beim Datei-Server sollten Benutzerdaten und Betriebssystem unbedingt in getrennten Partitionen liegen.

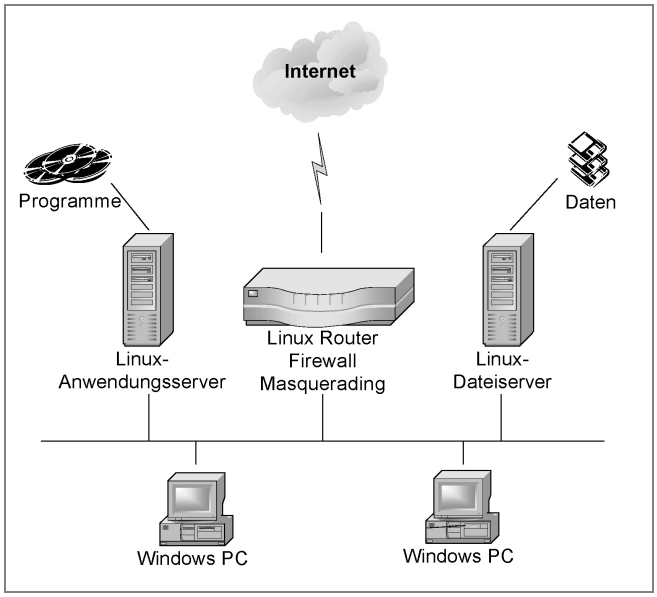

Abbildung 2.2: Verteilte Linux-Server

Vielen Unternehmen und Organisationen wachsen die laufenden Kosten der Betreuung von Windows-PCs über den Kopf. Sie starten deshalb Endgeräte von zentralen Bootservern oder verlagern ganze PCs und Anwendungen auf zentrale virtuelle PCs oder Anwendungs-Server. An den Arbeitsplätzen nutzen sie dabei nur Anzeigegeräte (Thin-Clients) wie Windows-Terminals, Linux-Terminals, Diskless Linux oder Flash-ROM-Linux-PCs (siehe dazu den zweiten Teil dieses Buchs).

Sollen Anwender an Terminals sowohl X11-Programme als auch Windows-Programme nutzen, benötigt man einen Anwendungs-Server für X11-Anwendungen und eine Lösung für Windows-Anwendungen (Abbildung 2.3).

Windows-Anwendungen können dabei u. a.

- auf virtuellen Windows-Maschinen in einer Virtualisierungs-Lösung wie VMWare,
- auf Windows-Servern mit Terminalserver-Funktion
- oder in einer Windows- Ablaufumgebung wie Crossover Office

betrieben werden. In den ersten beiden Fällen kommunizieren die Endgeräte mit den Servern über Microsofts proprietäres Remote Desktop Protocol (RDP).

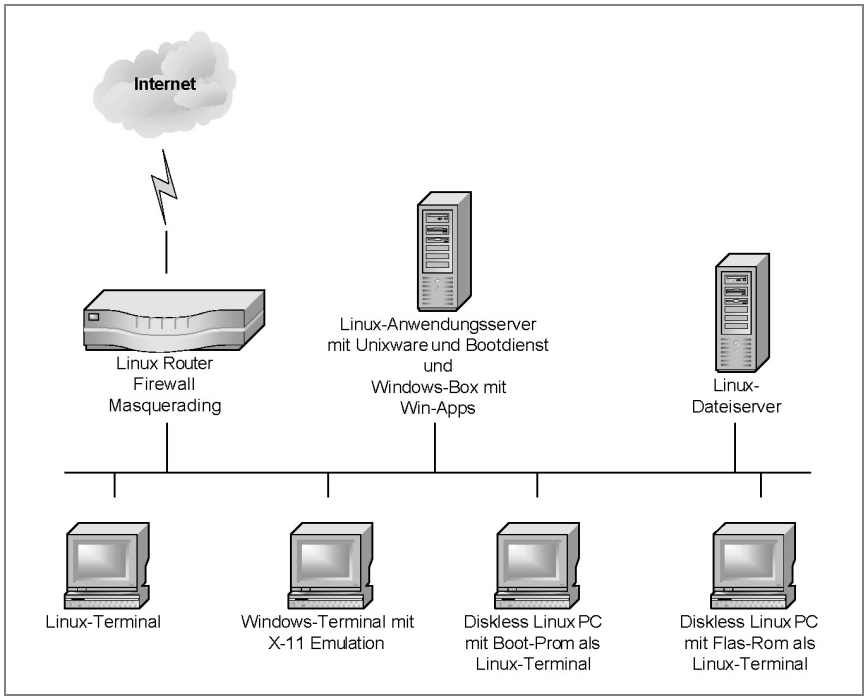

Abbildung 2.3: Windows-Anwendungen für Terminals

2.3 Festplatten vorbereiten

2.3.1 Dateisysteme

Bevor Sie Festplatten partitionieren, sollten Sie sich für geeignete Dateisysteme entscheiden. Während Windows-Server nur NTFS bieten, können Sie bei Linux-Rechnern zwischen verschiedenen Lösungen wählen, u. a.

- `Ext2`
- `Ext3`
- `Reiserfs`
- `XFS`

Das Dateisystem `Ext2` war lange das klassische Linux-Dateisystem. Bei wachsender Festplattengröße dauern aber die Integritätstests immer länger, die nach einer bestimmten Betriebszeit oder nach ungeplantem Herunterfahren der Rechner erforderlich sind. Der Test kann leicht mehr als eine halbe Stunde dauern – selbst bei einer aus heutiger Sicht kleinen Festplattengröße von 40 GByte.

Dagegen pflegen Journaling-Dateisysteme wie `Ext3` und `Reiserfs` ein zusätzliches Journal mit den Veränderungen, um im Notfall anhand dieses Journals das Dateisystem sehr schnell wieder herstellen zu können.

OpenSUSE setzt bei der Standardinstallation auf `Ext3` und nicht mehr auf `Reiserfs`, das SUSE einst mit vorangetrieben hat.[1]

Ein großer Vorteil von `Ext3` besteht darin, dass es zu `Ext2` aufwärtskompatibel ist. Eine `Ext2`-Partition lässt sich ohne Datenverlust zu `Ext3` konvertieren, es muss nur nachträglich das Journal erzeugt und aktiviert werden. Notfalls lässt sich eine `Ext3`-Partition auch im `Ext2`-Modus einbinden, was das Starten von Rettungssystemen erleichtern kann. Außerdem gibt es deutlich mehr Tools für das Sichern und Wiederherstellen von `Ext2` als für `Reiserfs`.

Sehr gute Kritiken gibt es seit einiger Zeit für das Dateisystem `XFS` der Firma SGI.

Sie können aber in jedem Fall bedenkenlos den Vorschlägen von YaST folgen und auf das Dateisystem `Ext3` setzen.

2.3.2 Partitionieren der Festplatte

Vor dem Installieren sollten Sie die Aufteilung der Festplatten detailliert planen, weil diese u. a. für die Sicherheit Ihrer Server von Bedeutung ist und sich diese später nur mühsam ändern lässt.

Die Standardinstallation von OpenSUSE teilt Festplatten z. B. folgendermaßen auf, wobei die Kapazitätsangaben von der Größe Ihrer Festplatte abhängen und die Kapazität der Swap-Partition vom Umfang des Hauptspeichers. Die Angaben beziehen sich auf eine IDE-Festplatte; für ein SCSI-System steht statt `hda` jeweils `sda`:

Device-Name	*Kapazität*	*Mount-Point*	*Bedeutung*
`/dev/hda2`	restliche Kapazität	`/`	Rootpartition (Reiserfs)
`/dev/hda1`	1 GB		Swap-Partition

Tabelle 2.1: Partitionen der Festplatte

Auf reinen Linux-Servern werden Sie kaum Windows-Partitionen wie FAT oder NTFS benötigen. Sollten Sie auf einem Linux-Server dennoch eine Windows-Partition eingerichtet haben, so verschieben sich dadurch die Nummern der Linux-Partitionen hinter die Windows-Partitionen.

Die eigentliche Linux-Installation befindet sich bei der Standardaufteilung in der Partition `/dev/hda2`. Während dies für Desktop-Rechner unproblematisch ist, müssen Sie auf Serversystemen mit vielen Benutzern damit rechnen, dass die Benutzer große Daten-

[1] Die Zukunft des Reiser-Dateisystems ist zunehmend fraglich, da dessen Schöpfer Hans Reiser wegen der Tötung seiner Ex-Frau eine langjährige Haftstrafe in den USA verbüßt.

mengen in ihren Home-Verzeichnissen ablegen. Haben Sie bei einem Server, der alle Serverdienste anbietet, nur eine einzige Partition angelegt, geht dem Linux-System der Speicherplatz aus, sobald Benutzer ihre Home-Verzeichnisse zu sehr füllen. Wenn der Speicherplatz vollkommen erschöpft ist, können einzelne Dienste oder das ganze System ausfallen.

Aus Sicherheitsgründen sollte man die Festplatte in mehrere Partitionen unterteilen, auch wenn man getrennte Anwendungs- und Dateiserver betreibt.

Systembetreuer können beim Installieren von OpenSUSE über den Menüpunkt *Erweiterte Einstellungen* • *manuelles Partitionieren* die Aufteilung der Festplatten selbst steuern.

Wenn Sie von Hand partitionieren wollen, so sollten Sie das mit YaST oder mit dem Programm `fdisk` aus einem Rettungssystem heraus machen. Eine Empfehlung für das Partitionieren ist:

Partition	*Beschreibung*
Erweiterte Partition mit der restlichen Kapazität der Festplatte	Auf einer Festplatte kann man nur vier primäre (oder erweiterte) Partitionen anlegen. Das ist für diese Aufteilung nicht genug. Will man weitere Partitionen einrichten, so kann man diese innerhalb einer erweiterten Partition als logische Partition anlegen. Die Nummerierung der logischen Partitionen beginnt mit `/dev/hda5`.
Swap-Partition 1 GB, bzw. das Doppelte des vorhandenen Hauptspeichers (logisch `/dev/hda5`)	Die Swap-Partition dient als virtueller Arbeitsspeicher. Wenn Sie viele speicherhungrige Anwendungen parallel laufen lassen, dann kann Linux hierher Speicherinhalt auslagern. Auf eine Swap-Partition sollte man daher auch bei umfangreichem Arbeitsspeicher nicht verzichten. Die Arbeitsgeschwindigkeit von virtuellem Speicher ist aber erheblich niedriger als die des tatsächlichen Hauptspeichers.
`/` 5-10GB (logisch `/dev/hda6`)	Die Größe der Root-Partition sollte zwischen 5 GB und 10 GB liegen. Der konkrete Wert hängt davon ab, wie viel Software Sie auf dem System installieren wollen. Bei der hier im Buch beschriebenen Installation kämen Sie mit 3 GB gerade aus. Wenn Sie speicherhungrige Anwendungen wie OpenOffice.org installieren, benötigen Sie mehr Speicherplatz, vor allem im Verzeichnis `/opt`. Daher sind 10 GB meist eine sichere Wahl. Bei Bedarf können Sie auch für das Verzeichnis `/opt` eine extra Partition einrichten. Die Daten für den Web-Server Apache legt man üblicherweise im Ordner `/srv/www/htdocs` ab. Wenn Sie ein sehr umfangreiches Webangebot planen, sollten Sie für diesen Ordner eine eigene Partition einplanen.

Partition	*Beschreibung*
`/tmp` 1 GB (logisch `/dev/hda7`)	Im Verzeichnis `/tmp` legen verschiedene Programme kurzfristig Daten ab. Sie sollten diese Partition daher nicht kleiner anlegen. Falls Sie mit mehreren Benutzern und KDE arbeiten kann die Partition ruhig etwas größer werden, da KDE viele temporäre Daten anlegt.
`/var` 5 GB (logisch `/dev/hda8`)	Im Verzeichnis `/var` liegt das Unterverzeichnis `/var/spool`, in dem sehr viele Daten abgelegt werden, z. B. die eingehenden Mails in `/var/spool/mail`. Für diese Daten müssen Sie ausreichend Speicherplatz zur Verfügung stellen. Falls Sie mit *cyrus-imap* arbeiten, benötigen Sie innerhalb von `/var/spool` sogar 100MB pro Benutzer.
`/home` sehr viel (logisch `/dev/hda9`)	In dieser Partition liegen die Home-Verzeichnisse der Benutzer. Sie sollten hier genügend Kapazität vorsehen.

Tabelle 2.2: Partitionierungsempfehlung

Die folgende Tabelle fasst obige Vorschläge fürs Partitionieren zusammen:

Partition	*Kapazität*	*Mount-Point*	*Inhalt*
`/dev/hda1`	gesamte Kapazität		Erweiterte Partition
`/dev/hda5`	1 GB		Swap-Partition
`/dev/hda6`	5 – 10 GB	`/`	Root
`/dev/hda7`	1 GB	`/tmp`	temporäre Daten
`/dev/hda8`	5 GB	`/var`	u. a. Log- und Spooldateien
`/dev/hda9`	Rest	`/home`	Home-Verzeichnisse

Tabelle 2.3: Übersicht der Partitionen

Wenn Sie den Speicherplatz für einzelne Programme oder Dienste beschränken wollen, sollten Sie weitere Partitionen einrichten. Im Kapitel 3.3 lesen Sie, wie Sie obendrein mit Disk-Quotas den Speicherplatz in den Home-Verzeichnissen Ihrer Benutzer beschränken können. Wollen Sie auch den Speicherplatz für eingegangene und noch nicht abgerufene Mails (`/var/spool/mail`) beschränken, so legen Sie hierfür am einfachsten eine eigene Partition an oder richten auch hierfür Disk-Quotas ein.

2.3.3 RAID

Vorbemerkung

Für kommerzielle Datenhaltung benötigt man redundante und schnelle Speicherlösungen. Bewährt haben sich verschiedene Level von Raid (Redundant Array of Independent Disks).

Raid – verständlich erklärt

Die wichtigsten Raid-Kategorien sind:

- Raid 0 fasst zwei oder mehr Festplatten zu einem so genannten Stripe-Set zusammen und verteilt Schreib- und Lesezugriffe auf mehrere Platten, um den Zugriff zu beschleunigen. Raid 0 bietet keinerlei Sicherheit. Ist auch nur eine Platte des Arrays defekt, so sind alle Daten verloren. Dafür erfolgen die Festplattenzugriffe deutlich schneller als bei Lösungen ohne Raid oder bei Raid 1, da die Platten parallel arbeiten können.
- Raid 1 spiegelt Festplatten (Mirroring). Es schreibt alle Daten auf zwei physikalisch verschiedene Platten. Fällt eine Platte aus, kann man mit der anderen Platte weiterarbeiten. Sind die jeweiligen Partitionen auf beiden Festplatten verschieden groß, kann man nur so viel Speicherplatz nutzen, wie die kleinere Partition besitzt.
- Raid 5 beschreibt ein Stripe-Set ähnlich Raid 0, das zusätzlich Parity-Informationen sichert. Für Raid 5 sind mindestens drei Platten beziehungsweise Partitionen erforderlich. Fällt eine Platte aus, so können mit den Parity-Informationen die Daten wiederhergestellt werden. Bei Raid 5 mit drei (n) Platten steht das Doppelte ((n-1)-fache) der kleinsten Platte für Nutzdaten zur Verfügung.

Traditionell verwendet man unabhängig vom Server-Betriebssystem Hardware-Raid, um Daten redundant und schnell zu speichern und zu lesen. Während hierfür bisher nur relativ teure SCSI-Lösungen zur Verfügung standen, sind jetzt IDE/ATA-Lösungen günstig verfügbar (z. B. `www.3ware.com`). Ist überhaupt kein Budget für Hardware-Raid-Systeme vorhanden, kann man Software-Raid Level 1 oder 5 einrichten.

Wenn Sie für Ihre Daten einen gesonderten File-Server betreiben wollen, ohne in Raid-Controller zu investieren, können Sie Ihre Daten bei Linux mit Software-Raid der `raidtools` spiegeln.

2.4 Linux für Serverdienste installieren

Im einfachsten Fall nimmt man bei der OpenSUSE-Distribution eine Standardinstallation vor und ergänzt fehlende Programme beim Konfigurieren. Lediglich die Partitionierung sollten Sie Ihren Bedürfnissen anpassen.

An vielen Stellen dieses Buchs wird auf die Standardinstallation und Konfiguration mit YaST, dem Konfigurationstool von OpenSUSE, zurückgegriffen.

Der prinzipielle Ablauf der Installation des Linux-Servers besteht aus folgenden Schritten:

1. Booten von DVD: Die OpenSUSE-DVD ist bootfähig. Falls Ihr Rechner nicht von der DVD startet, müssten Sie vielleicht noch im BIOS die Bootreihenfolge verändern.

2. Partitionieren der Festplatte: Zum Partitionieren der Festplatte haben Sie im vorangegangenen Abschnitt schon Anregungen erhalten.
3. Installation ausgewählter Pakete: Zur Distribution OpenSUSE 11.0 gehören etwa 6.000 Software-Pakete. Für eine sinnvolle Konfiguration, wie sie dieses Buch beschreibt, benötigen Sie etwa 500 Pakete. Um die Auswahl zu erleichtern, hat OpenSUSE ein *Standardsystem* zusammengestellt, das Sie für den Anfang installieren sollten.
4. Konfiguration: Ein großer Teil der Programme ist sofort nach der Installation lauffähig, andere muss man erst konfigurieren. Wollen Sie die Kapitel dieses Buchs nachvollziehen, sollten Sie sogleich einzelne hier genannte Pakete nachträglich installieren, die nicht zum *Standardsystem* gehören.

Sie sollten bei der Installation möglichst mit den Vorgaben von OpenSUSE arbeiten. Die meisten Einstellungen können Sie auch noch später bei Bedarf anpassen. Lediglich die Partitionierung lässt sich hinterher nur sehr schwer verändern.

Die Beschreibungen verwenden den Rechnernamen `boss` und die Domäne `lokales-netz.de`. Die Domäne `lokales-netz.de` haben die Autoren beim DENIC reserviert, Sie können sie also problemlos als Beispiel für Ihre Konfiguration benutzen. Sollten Sie bereits über eine eigene Domain verfügen, so ersetzen Sie einfach in allen Beispielen `lokales-netz.de` durch Ihre eigene Domain. Der Rechnername `boss` ist willkürlich. Es ist aber sinnvoll, Namen zu nehmen, die in den alphabetisch sortierten Listen der Windows-Umgebung weit oben stehen, damit sie in der Netzwerkumgebung ganz oben auftauchen und man sie nicht erst hinter 234 Clients findet.

Der Server hat hier in den Beispielen die IP-Adresse `192.168.1.2`. Der Adressbereich `192.168.1.xx` gehört zu den privaten Netzadressen, die niemals offiziell vergeben werden. Daher können Sie diesen Adressbereich gut in lokalen Netzen benutzen, ohne dass er im Internet auftaucht. Die Zuordnung der konkreten IP-Adresse zum Server ist beliebig. Die Auswahl der `2` soll dies deutlich machen.

Für die Verteilung der IP-Adressen im Netz sollten Sie sich ein System überlegen. Die Beispiele im Buch benutzen die IP-Adressen unterhalb von 10, also `192.168.1.1` bis `192.168.1.9` für besondere Geräte, wie den Linux-Server und Print-Server. Die Windows-Clients nutzen IP-Adressen ab 10.

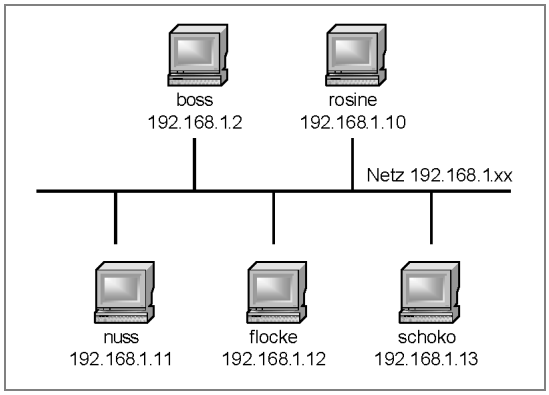

Abbildung 2.4: Beispielnetzwerk

Um das Einbinden des Linux-Servers in das Windows-Netz zu erleichtern, sollten Sie auf dem Linux-Server möglichst bald die Serverprogramme für *DHCP* (Kapitel 2.6) und *POP3* (Kapitel 2.7) einrichten, die als sogenannte Dämonen ständig im Hintergrund laufen und auf Anfragen warten. Der DHCP-Server verteilt dynamisch IP-Adressen im Netz und der POP-Dämon die elektronische Eingangspost an registrierte Benutzer.

2.5 Pakete nachinstallieren

Im vorangegangenen Abschnitt konnten Sie die Empfehlung lesen, möglichst mit einer Standardinstallation zu beginnen, um später eventuell fehlende Programmpakete nachzuinstallieren.

Für die Installation können Sie mit unterschiedlichen Versionen der Distribution beginnen:

- Mit der Kaufversion, die in Online- oder Laden-Buchhandlungen vertrieben wird.
- Mit der freien Datenträgerversion, von der Sie die DVD bzw. CD-Images kostenlos über `http://software.opensuse.org/` laden und auf einen Datenträger brennen können.
- Mit der Online-Version (siehe Abschnitt 2.5.3), bei der die Installation ihre Quellen weitgehend direkt über das Internet bezieht.

In allen Versionen finden Sie die hier im Buch beschriebenen Pakete.

Sollten Sie bei einer Version ein Paket vermissen, können Sie es über eine Internetverbindung leicht von der folgenden URL laden:

`http://download.opensuse.org/distribution/11.0/`.

Sollten die OpenSUSE-Server einmal sehr überlastet sein, haben Sie bei der Gesellschaft für wissenschaftliche Datenverarbeitung in Göttingen vielleicht mehr Glück:

```
ftp://ftp.gwdg.de/pub/opensuse/distribution/11.0/
```

Pakete können Sie auf verschiedenen Wegen nachinstallieren:

- über die grafische Variante von YaST und die Paketauswahl der CD/DVD,
- die textbasierte Version von YaST,
- oder direkt über einen FTP-Server.

2.5.1 Installation von CD/DVD mit YaST

Mit dem Konfigurations-Tool YaST können Sie u. a. Software-Pakete installieren. Sie finden das Icon zum Start des YaST-Kontrollzentrums an mehreren Stellen im Menübaum. Eine einfache Möglichkeit besteht darin, auf das erste Icon der KDE-Funktionsleiste zu klicken (*K-Menü*) und dann im Menü auf *System*. Hier finden Sie YaST als unterstes Icon.

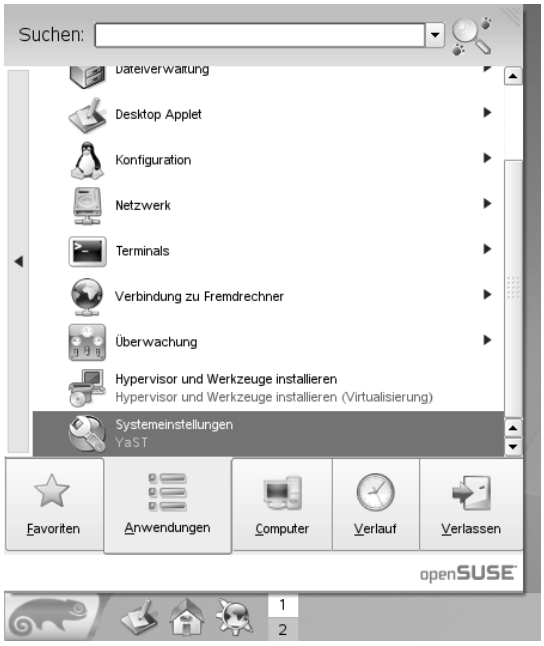

Abbildung 2.5:
YaST-Kontrollzentrum in KDE

Über die anderen Menüpunkte können Sie die einzelnen Funktionen von YaST auch getrennt aufrufen. Dieses Buch geht davon aus, dass Sie immer zuerst das Kontrollzentrum starten und von dort aus die einzelnen Funktionen aufrufen.

Das YaST-Kontrollzentrum startet dann mit folgender Darstellung:

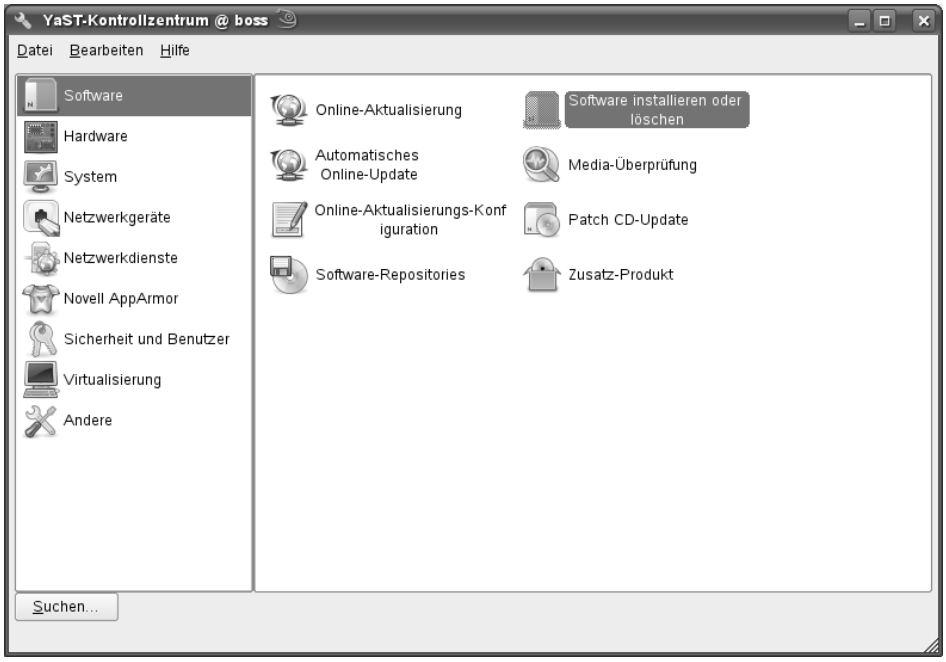

Abbildung 2.6: YaST

Wenn Sie dann in der Rubrik *Software* den Punkt *Software installieren oder löschen* auswählen, öffnet YaST einen Dialog zur Paketauswahl.

Sie können hier Pakete mit unterschiedlichen Filtern auswählen. Der Standardfilter, die Suchfunktion, erleichtert das Stöbern nach Paketen. Für die Beschreibungen im Buch benutzen wir oft den Filter *Paketgruppen*; am häufigsten benötigen Sie die Selektion *Netzwerk* für die Programmpakete für Serverdienste. Daneben gibt es noch den Filter *Schemata*, der alle Pakete nach formalen Kriterien auflistet. Dieses Buch zeigt von den drei Möglichkeiten jeweils die einfachste.

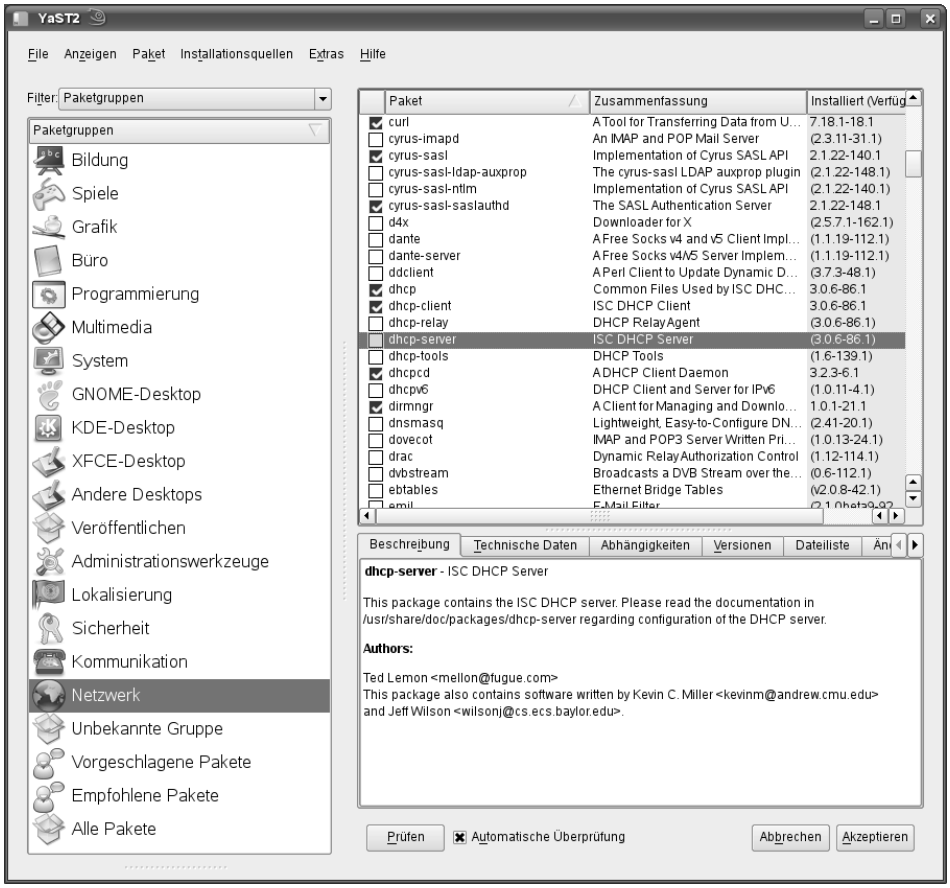

Abbildung 2.7: YaST: Paketauswahl

Der rechte Teil des Formulars zeigt immer die Pakete, auf die die Filterkriterien zutreffen. Die Icons vor den Paketbezeichnungen geben den Status eines Pakets an.

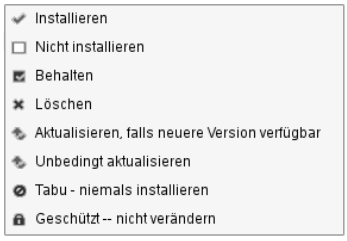

Abbildung 2.8: YaST: Paketstatus

Die wichtigsten Optionen sind hier:

- Löschen (rotes X),
- Installieren (angewählte Checkbox),
- Automatisch installieren (wie Installieren, aber mit schwarzem Dreieck davor) und
- Nicht installieren (leere Checkbox).

Oft benötigen von Ihnen ausgewählte Pakete ihrerseits weitere Pakete. YaST erkennt solche Abhängigkeiten selbstständig und installiert die notwendigen Pakete automatisch mit. Automatisch ausgewählte Pakete erkennen Sie an den Icons mit einem vorangestellten Dreieck.

Zur Auswahl eines Pakets müssen Sie nur die zugehörige Checkbox aktivieren und am Ende des Dialogs auf *Übernehmen* klicken. YaST fordert Sie dann zum Einlegen des passenden Mediums auf.

2.5.2 Installation von CD/DVD im Textmodus

Sie können YaST auch ohne grafische Oberfläche nutzen, entweder direkt von der Konsole, oder auch übers Netz mit einer Telnet- oder besser einer SSH-Verbindung. Weitere Informationen zu Telnet und SSH finden Sie im Kapitel 5.

Die Benutzerschnittstelle der textbasierten Version von YaST ist spartanischer und etwas umständlicher zu bedienen, da sie ohne Maus auskommen muss. Dafür ist die Bedienung deutlich schneller, wenn Sie sich an die Tastenkürzel gewöhnt haben.

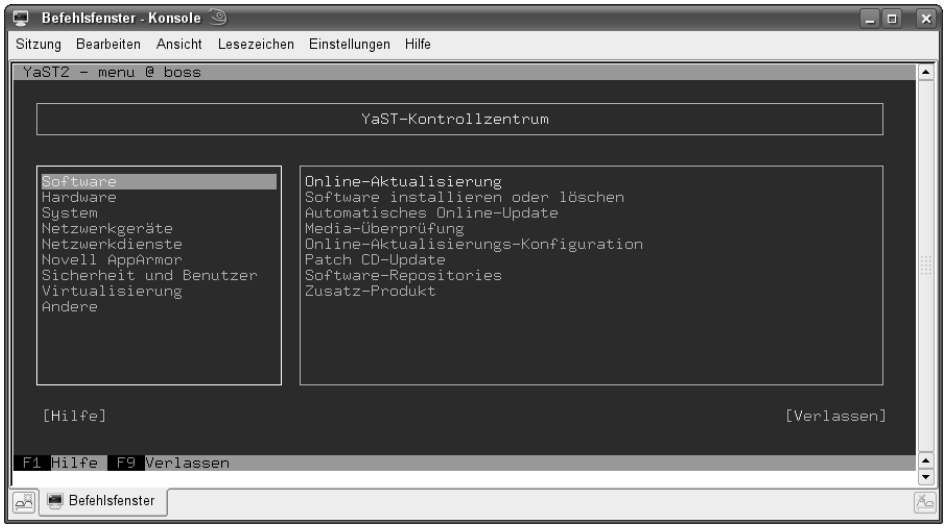

Abbildung 2.9: YaST: Textversion

Hier können Sie sich mit der `Tab`-Taste und den `Cursor`-Tasten durch die Funktionen hangeln oder mit der `ALT`-Taste und dem hervorgehobenen Buchstaben direkt eine Funktion auswählen. Mit `ALT+V` können Sie z. B. YaST direkt verlassen.

YaST lässt Sie hier mit den gleichen Filtern die gewünschten Pakete auswählen.

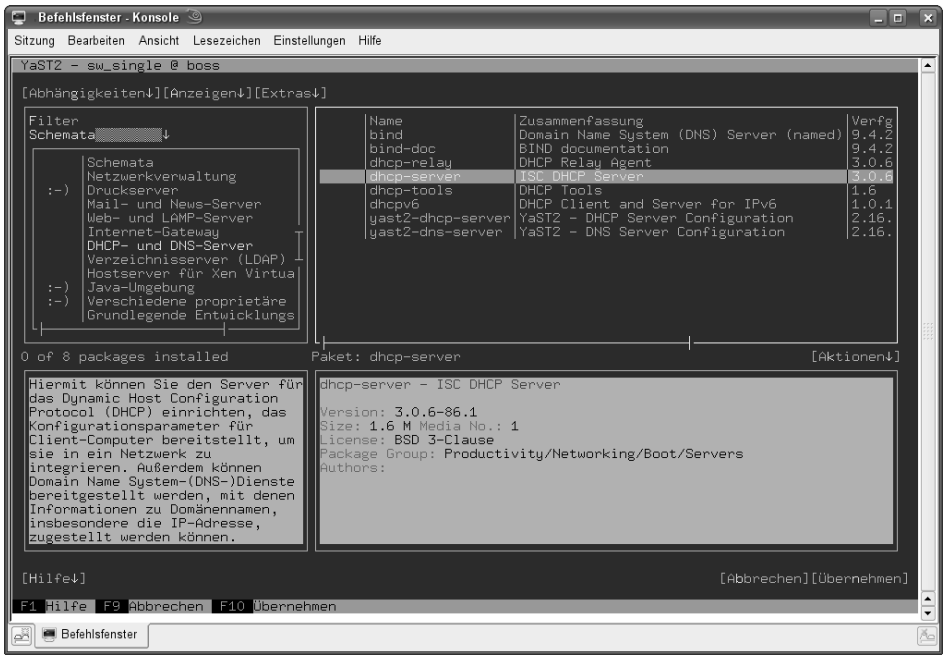

Abbildung 2.10: YaST: Textversion DHCP-Server

Zwar stellen manche SSH- oder Telnet-Clientprogramme bei Verbindungen übers Netzwerk einige Sonderzeichen falsch dar, doch dies beeinträchtigt die Funktionalität von YaST nicht.

2.5.3 Installation vom FTP-Server

Wenn Sie ein von Ihnen gewünschtes Paket nicht auf den Medien der Distribution finden, können Sie es von einem FTP-Server laden.

Die eigentlichen Pakete liegen als einzelne Dateien vor. Deren Namen enden auf `.rpm` und beinhalten vor der Endung eine Versionsbezeichnung sowie die Prozessorfamilie. Das Paket `dhcp-server` finden Sie also z. B. in der Datei `dhcp-server-3.0.6-86.1.i586.rpm`. Die Version 3.0.6 des Pakets ist somit für Pentium-Prozessoren der Prozessorfamilie i586 kompiliert.

Hinweis: OpenSUSE fasst sämtliche Komponenten eines Programms in einer einzigen komprimierten Datei im Dateiformat des Red Hat Package Manager (rpm) zusammen. Zur Vereinfachung der Installation pflegt und verwaltet der Paketmanager eine Datenbank mit allen installierten Paketen.

Wenn Sie die Datei von einem der FTP-Server beziehen, kopieren Sie die jeweilige `rpm`-Datei zunächst mit dem Befehl `wget` in das Verzeichnis `/tmp`

```
cd  /tmp
wget
http://download.opensuse.org/distribution/11.0/repo/oss/suse/i586/dhc
p-server-3.0.6-86.1.i586.rpm
```

und installieren die Datei von dort aus mit dem Befehl

```
rpm  -i   /tmp/ dhcp-server-3.0.6-86.1.i586.rpm
```

Der Schalter `-i` weist den Package Manager an, das angegebene Paket zu installieren.

RPM löst Abhängigkeiten nicht automatisch auf. Fehlen Pakete, meldet RPM dies als Fehler und führt die Installation nicht aus. In diesem Fall müssen Sie zuerst die von RPM genannten fehlenden Pakete laden und installieren.

Das Download-Programm `wget` ist in allen Installationen vorhanden, da YaST es für sein eigenes Online-Update benötigt.

Da der Red Hat Package Manager Dateien direkt von FTP-Servern beziehen kann, können Sie Programme stattdessen auch in einem einzigen Schritt fernladen und installieren,

```
rpm  -ivh
http://download.opensuse.org/distribution/11.0/repo/oss/suse/i586/dhc
p-server-3.0.6-86.1.i586.rpm
```

Der Parameter `-i` veranlasst das Installieren des Pakets, `-v` (verbose) zeigt ausführlichere Meldungen und `-h` einen Fortschrittsbalken während der Installation des Pakets, wie bei der Installation mit YaST.

Der Dateimanager und Webbrowser Konqueror hilft bei der Installation von RPM-Paketen:

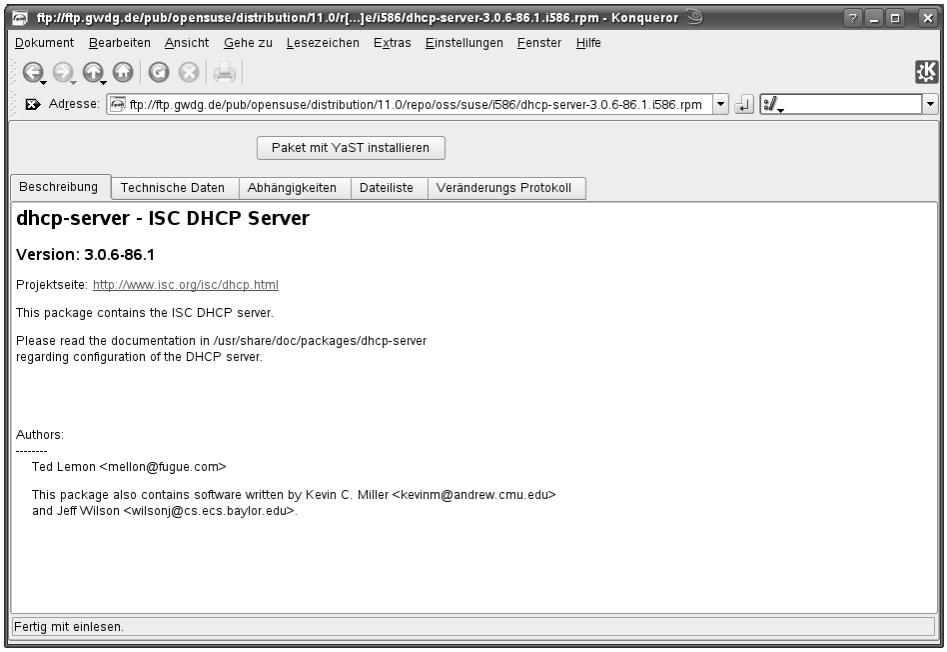

Abbildung 2.11: Konqueror: RPM-Installieren

Wenn Sie im Konqueror eine RPM-Datei aufrufen, zeigt er die Paketinformationen und bietet an, dieses Paket mit YaST zu installieren. Das ist vor allem bei Paketen nützlich, die nicht zum Lieferumfang der Distribution gehören.

2.5.4 Internetinstallation

Verfügen Sie über eine schnelle und preiswerte Internetanbindung, dann können Sie OpenSUSE auch direkt aus dem Internet installieren. Sie müssen dazu zuerst ein Boot-Image vom FTP-Server laden und damit nach Anleitung eine Boot-CD erstellen. Wenn Sie Ihren Rechner mit dieser Boot-CD starten, können Sie als Installationsmedium den Server `download.opensuse.org` (IP-Adresse: `195.135.221.130`) und das Verzeichnis `/pub/opensuse/distribution/SL-OSS-factory/inst-source/` angeben und so auch die Grundinstallation durchführen.

2.6 Adressen dynamisch verteilen

In IP-Netzen müssen sich Rechner mit einer eindeutigen Adresse ausweisen.

Generell gibt es zwei Möglichkeiten, IP-Adressen im lokalen Netz zu verteilen:

- feste Adressen per Individualeintrag und
- dynamische Adressen per DHCP.

Bei der ersten Methode gibt man jeden Rechner individuell eine feste IP-Adresse. Dieses Verfahren erfordert eine gute Übersicht und Dokumentation, da niemals zwei Rechner mit der gleichen IP-Adresse im Netz aktiv sein dürfen.

Einfacher zu verwalten ist eine automatische Adress-Zuordnung per DHCP (*Dynamic Host Control Protocol*). Hierfür benötigt man einen DHCP-Server, der anderen Geräten im Netz, also auch den Windows-Rechnern, IP-Adressen dynamisch zuteilt.

Die Zuordnung einer IP-Adresse zu einem Rechner bezeichnet man als Ausleihe (lease). Um Doppelausleihen auszuschließen, vermerkt der DHCP-Dämon (DHCPD) seine Ausleihen in der Datei `/var/lib/dhcp/dhcpd.leases`. Jede Ausleihe besitzt eine einstellbare Gültigkeit (*lease-time*). Dadurch kann man erreichen, dass der DHCPD den Windows-Rechnern jedes Mal die gleiche IP-Adresse zuordnet.

Einen DHCP-Server können Sie auf Ihrem DSL-Internet-Modem beziehungsweise Router oder auf Ihrem Linux-Server betreiben. Auf dem Linux-Server muss man den DHCP-Server nachträglich installieren, da die Standardinstallation ihn nicht einrichtet.

Der DHCP-Server befindet sich in der Paketgruppe `Netzwerk` im Paket `dhcp-server`.

Wollen Sie den DHCP-Server auch mit YaST konfigurieren, so müssen Sie zusätzlich das Paket `yast-dhcp-server` installieren, welches am einfachsten über den *Suchen*-Filter zu finden ist.

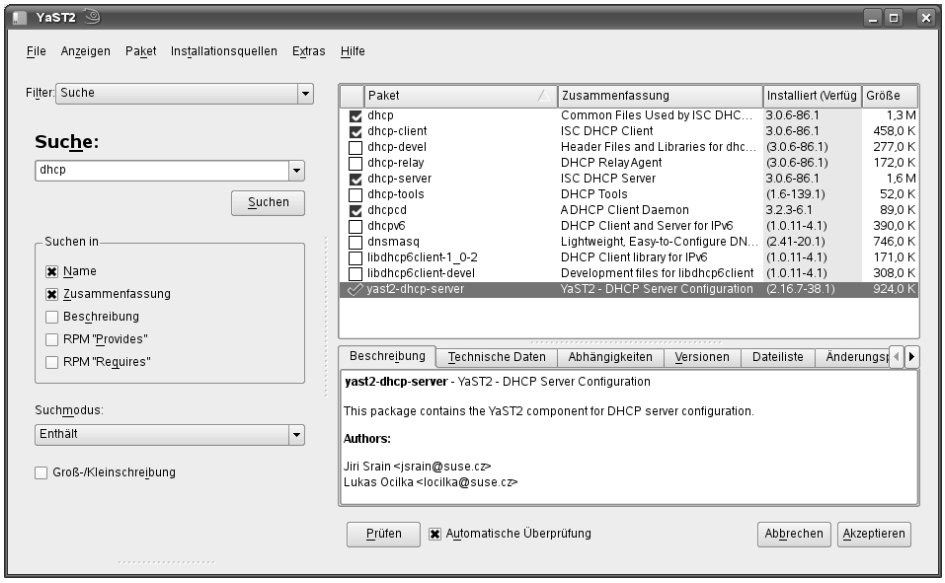

Abbildung 2.12: YaST: DHCP-Server installieren

Nach der Installation muss man die Konfigurationsdatei `/etc/dhcpd.conf` erstellen. Am einfachsten arbeiten Sie dazu weiterhin mit YaST. Falls Sie das Paket `yast-dhcp-server` neu installiert haben, müssen Sie YaST aber erst neu starten, um die zugehörige Funktion nutzen zu können.

YaST ermittelt im ersten Schritt der Konfiguration die verfügbaren Netzwerkkarten des Servers, auf dem der DHCP-Server hier läuft, und bietet sie Ihnen zur Auswahl an.

Abbildung 2.13: YaST: DHCP-Server Konfiguration 1

Das hier ausgewählte Interface trägt YaST in die Datei `/etc/sysconfig/dhcp` ein.

`/etc/sysconfig/dhcp` (Dateianfang)

```
## Path:        Network/DHCP/DHCP server
## Description: DHCP server settings
## Type:        string
## Default:     ""
## ServiceRestart: dhcpd
#
# Interface(s) for the DHCP server to listen on.
#
# A special keyword is ANY, it will cause dhcpd to autodetect #
available interfaces.
#
# Examples: DHCPD_INTERFACE="eth0"
#           DHCPD_INTERFACE="eth0 eth1 eth2 tr0 wlan0"
#           DHCPD_INTERFACE="internal0 internal1"
#           DHCPD_INTERFACE="ANY"
#
DHCPD_INTERFACE="eth0"
…
```

Im nächsten Schritt geht es um die Namen und Adressen, die der DHCP-Server übermitteln soll, in der Regel seine eigenen.

Abbildung 2.14: YaST: DHCP-Server Konfiguration 2

Jetzt fehlen dem DHCP-Server noch Angaben, aus welchem Bereich er die IP-Adressen vergeben darf.

Wenn Sie dem Beispiel hier im Buch folgen, vergibt der Server die IP-Adressen aus dem Bereich `192.168.1.20` bis `192.168.1.200` und lässt die darüber und darunter liegenden Bereiche für Sonderaufgaben frei.

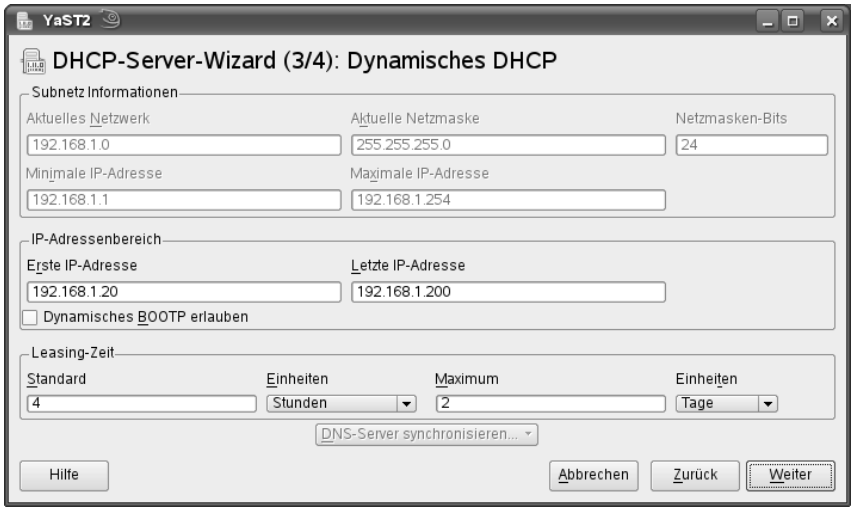

Abbildung 2.15: YaST: DHCP-Server Konfiguration 3

Bei den Leasing-Zeiten können Sie zunächst die Vorgaben übernehmen, bei denen jeder Client die von ihm ausgeliehene IP-Adresse alle 4 Stunden verlängern muss. Wenn eine Verlängerung nicht möglich ist, verfällt die Ausleihe spätestens nach 2 Tagen.

Im letzten Schritt der Konfiguration können Sie entscheiden, ob der DHCP-Server beim Systemstart mit starten soll, oder ob Sie ihn lieber manuell starten möchten. Außer in Testumgebungen sollte der DHCP-Server automatisch starten.

Wenn Sie in der letzten Maske auf *Beenden* klicken, ändert YaST die notwendigen Einstellungen und startet ggf. den DHCP-Server.

Die von YaST erzeugte Konfigurationsdatei hat, sofern Sie dem Beispiel gefolgt sind, folgenden Inhalt.

`/etc/dhcpd.conf`

```
option domain-name "lokales-netz.de";
option domain-name-servers 192.168.1.2;
option routers 192.168.1.2;
option netbios-name-servers 192.168.1.2;
ddns-update-style none;
default-lease-time 14400;
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.20 192.168.1.200;
  default-lease-time 14400;
  max-lease-time 172800;
}
```

Im ersten Teil stehen die allgemeinen Einstellungen, wie der Domain-Name, die Adressen der Nameserver und die Adresse des Routers. Weiter unten folgen die Lease-Zeiten (Ausleihzeiten bzw. Leasing-Zeiten bei YaST) für die IP. Die IP wird hier nach vier Stunden aktualisiert und verfällt nach zwei Tagen.

Soll der Client hingegen die Ausleihe nur noch einmal täglich mit einer maximalen Gültigkeit von einer Woche erneuern, damit er immer die gleiche IP anfordert (solange er nicht länger als eine Woche außer Betrieb ist), müssten Sie die Zeiten so ansetzen:

```
default-lease-time 86400;
max-lease-time 604800;
```

Die Zeile `ddns-update-style` enthält eine neue Funktion des DHCPD für die Windows-Namen der Clients:

```
ddns-update-style none;
```

Wenn Sie hier statt `none` den Wert `ad-hoc` angeben, kann der DHCPD die Windows-Namen der Clients gleich in den Nameserver eintragen. Das Kapitel 13 (Domain Nameserver einrichten) beschreibt diese Funktion ausführlich. So lange Sie Ihren Nameserver noch nicht konfiguriert haben, deaktivieren Sie die Funktion durch die Angabe `none`.

Anschließend folgen Einstellungen für das Netz.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.20 192.168.1.200;
  default-lease-time 14400;
  max-lease-time 172800;
}
```

Das Subnetz `192.168.1.0` verfügt über die Netzmaske `255.255.255.0`. Dies legt fest, dass alle Rechner, deren IP-Adressen sich nur in der letzten Zahl unterscheiden, zum gleichen Subnetz gehören. Der Server wählt die IP-Adressen aus dem Bereich `192.168.1.20` bis `192.168.1.200` und lässt die darüber und darunter liegenden Bereiche für Sonderaufgaben frei.

YaST hilft beim Erstellen einer Konfigurationsdatei mit den Grundeinstellungen. Wenn Sie aber weitere Parameter einstellen wollen, müssen Sie die Konfigurationsdatei direkt bearbeiten.

Wenn Sie z. B. für einen Printserver oder für Linux-Terminals mit spezieller Hardware (siehe Kapitel 10.2) einzelne IP-Adressen fest vergeben wollen, können Sie wie hier den Hardware-Adressen (MAC-Adressen) einzeln feste IP- Adressen zuordnen.

```
host printserver {
  hardware ethernet 08:00:07:26:c0:a5;
  fixed-address 192.168.1.7;
}
```

Hier bekommt z. B. ein Printserver eine feste IP-Adresse. Dazu benötigt DHCP die Hardware-Adresse von dessen Netzwerkkarte. Diese Hardware-Adressen stehen normalerweise auf dem Gehäuse derartiger Geräte. Der Printserver startet so immer mit seiner festen IP-Adresse. Der DHCP-Server erkennt ihn anhand seiner Hardware-Adresse.

Nachdem Sie mit

```
rcdhcpd start
```

den DHCP-Server aktiviert haben, sollten Sie auch die Windows-Rechner und sonstigen Clients Ihres lokalen Netzes neu starten. Wenn auf diesen die dynamische Adresszuteilung eingeschaltet war (siehe Kapitel 5.2), müsste der DHCP-Server diesen eine IP-Adresse zugewiesen haben.

Prüfen Sie sofort, ob das dynamische Zuordnen der IP-Adressen geklappt hat. Je nach Windows-Version brauchen Sie hierzu verschiedene Programme.

Bei Windows 9x-Rechnern ermitteln Sie die IP-Adresse mit *Start* • *Ausführen* und dem Befehl

```
winipcfg
```

Windows zeigt dann in einem kleinen Fenster die IP-Adresse des Rechners.

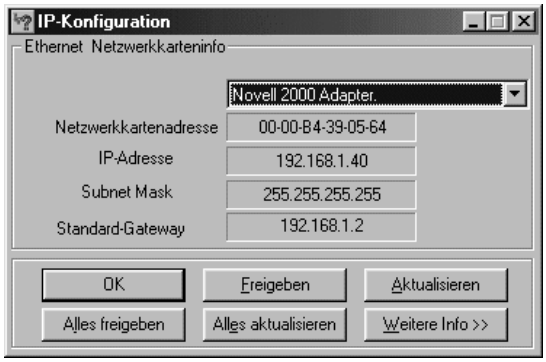

Abbildung 2.16:
Ausgabe von WinIPcfg

Wenn Sie hier eine korrekte IP für den Rechner sehen und auch die IP des Linux-Rechners richtig eingetragen ist, können Sie die IP-Verbindung nutzen.

Mit Windows Vista/XP/2000/NT rufen Sie mit dem Zubehör-Programm *Eingabeaufforderung* das Programm `ipconfig` mit dem Schalter `/ALL` auf, um alle Verbindungen zu sehen:

```
ipconfig   /ALL
```

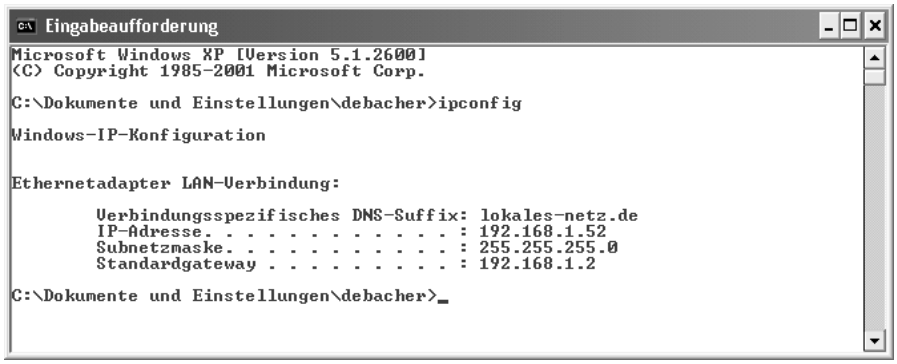

Abbildung 2.17: Ausgabe von ipconfig

Weitere Informationen zur Konfiguration der Windows-Clients finden Sie im Kapitel 5: Zugriff von Windows auf Linux-Server.

Sobald alles richtig funktioniert, sollte man auf dem Linux-Server den DHCP-Server automatisch beim Booten starten. Wenn Sie das bei der DHCP-Konfiguration nicht gleich eingestellt haben, können Sie jederzeit auch den Runlevel-Editor bemühen.

Sie finden im YaST-Kontrollzentrum unter *System* • *Runlevel-Editor* • *Experten-Modus* eine Auswahl aller Dienste, für die ein Startskript im Verzeichnis `/etc/init.d` vorliegt.

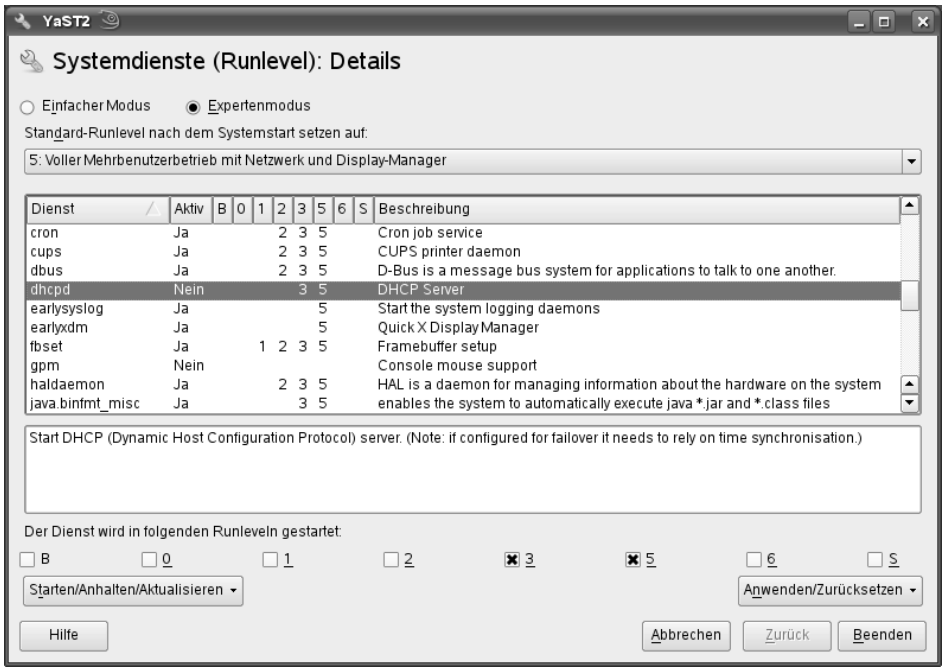

Abbildung 2.18: Aktivieren des DHCPD in YaST

Wenn Sie den Rollbalken auf die Zeile für den `dhcpd` führen und auf *Starten/Anhalten/Aktualisieren* • *Starten* klicken, führt YaST im Hintergrund den Befehl `dhcpd start` aus. Wenn Sie hier mit YaST arbeiten, sollten Sie für den `dhcpd` die Runlevel 3 und 5 auswählen.

2.7 Installation des POP-Dämons

Ihr Linux-Server kann für Linux- und Windows-Clients elektronische Post vermitteln.

Für das Abholen elektronischer Post auf dem Server gibt es mehrere Protokolle. Die bekanntesten davon sind POP3 (Post Office Protocol) und IMAP (Interactive Mail Access Protocol). Mit IMAP bearbeiten Sie Ihre Postablage im Ordner `/var/spool/imap` direkt auf dem Server, POP3 hingegen lädt die Nachrichten auf den lokalen Client und kann sie nach der Übertragung auf dem Server löschen.

Da POP3 für kleine lokale Netze vollkommen ausreicht, ist hier dessen Installation beschrieben. Ein geeigneter POP3-Dämon befindet sich im Paket `qpopper` in der Paketgruppe *Netzwerk*. Sie müssen dieses Paket nachträglich installieren.

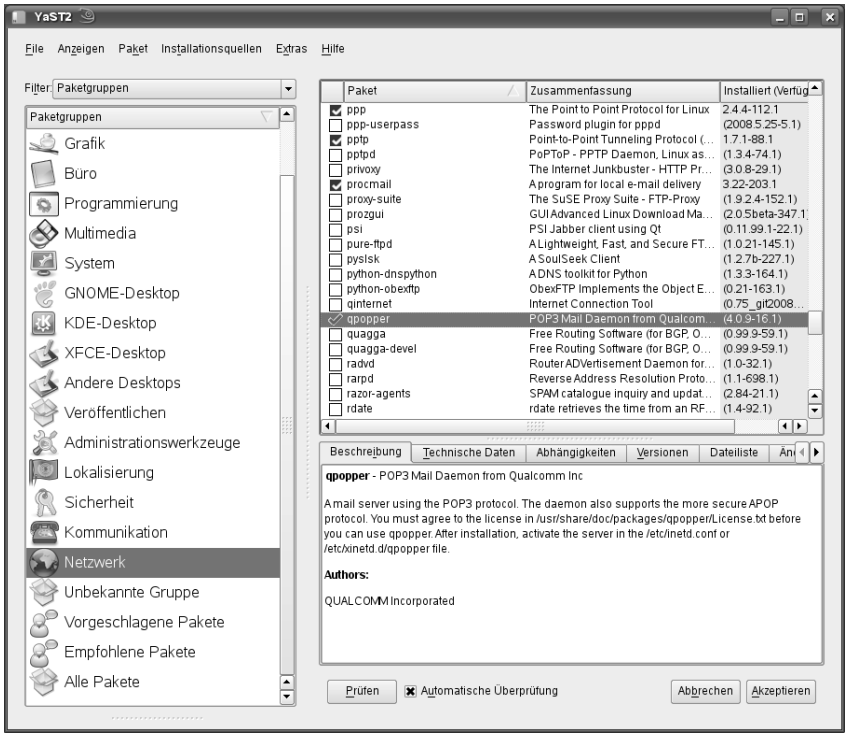

Abbildung 2.19: qpopper-Paketauswahl in YaST

Nach der Installation müssen Sie diesen Dienst noch aktivieren. Der POP3-Dämon ist kein eigenständiger Dienst wie der DHCP-Dämon. Um Systemressourcen zu sparen, ruft ihn der Superdämon `inetd` bzw. `xinetd` auf. Weitere Hinweise zu diesem Verfahren finden Sie im Kapitel »Vorgänge automatisch starten« im Abschnitt 4.4.

Hinweis: Das Paket `qpopper` unterliegt etwas abweichenden Lizenzbedingungen als die meisten anderen Pakete. Sie können es kostenlos nutzen, müssen aber mit den Lizenzbedingungen einverstanden sein, die Sie in der Datei `/usr/share/doc/packages/qpopper/License.txt` finden.

Den Dämon aktiviert man über das YaST-Kontollzentrum und die Funktion *Netzwerkdienste • Netzwerkdienste (xinetd)*. Sie sehen eine Liste aller vorbereiteten Dienste und deren Status.

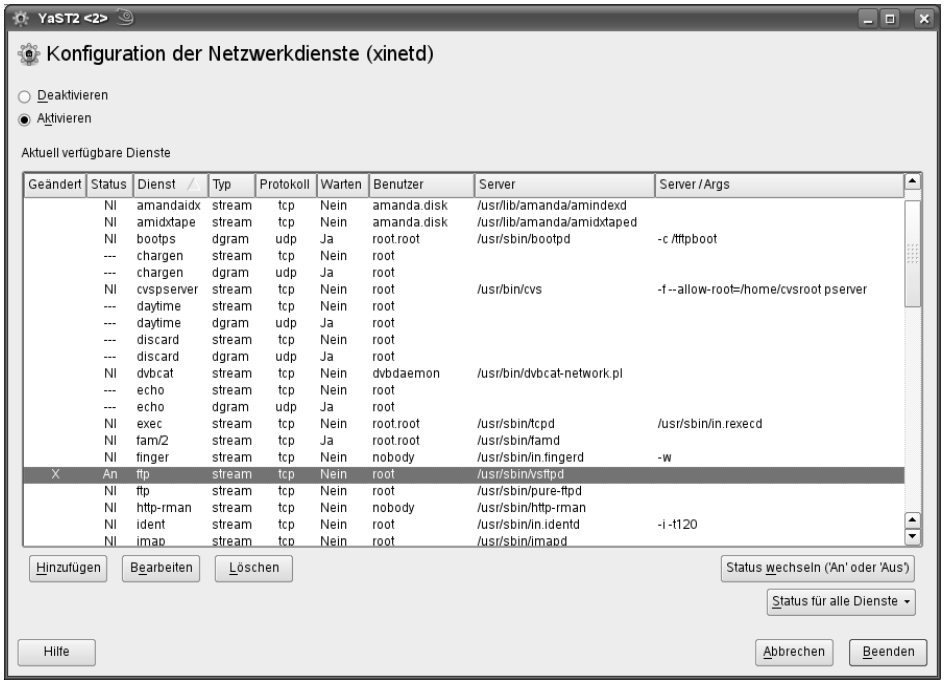

Abbildung 2.20: Aktivierung des qpopper

Im Auslieferungszustand ist keiner der Dienste eingeschaltet; OpenSUSE aktiviert den `xinetd` daher auch nicht. Sie müssen also im Zweifelsfall zuerst auf *Aktivieren* gehen, um den `xinetd` überhaupt zu starten.

Steuern Sie den Rollbalken auf den gewünschten Dienst, können Sie mit *Status wechseln* diesen Dienst aktivieren oder deaktivieren. Da YaST die Änderungen erst nach dem

Klick auf *Beenden* in die Konfigurationsdateien übernimmt, zeigt es in der ersten Spalte der Zeile noch an, dass es sich um eine geänderte Einstellung handelt.

Vorsichtshalber sollten Sie den `xinetd` nach Veränderungen an Diensten mit

```
rcxinetd  reload
```

veranlassen, seine Konfigurationsdateien neu einzulesen.

Nun können Sie auch von Client-Rechnern aus Nachrichten abrufen, die auf dem Server für Sie zur Verfügung stehen. Ausführliche Informationen zum Verteilen von E-Mails auf einem Linux-System finden Sie im Kapitel 14 »Email-Server«.

2.8 Informationen über Sicherheitsprobleme

Wenn Sie an Murphys Gesetz glauben, gibt es keine fehlerfreien Programme. Das betrifft leider auch die Linux-Welt, obwohl hier zumindest Systemabstürze selten sind. Viele Programme haben aber kleine Fehler, die sich im normalen Betrieb nicht bemerkbar machen. So können sie z. B. nur Eingaben von maximal 255 Zeichen Länge verkraften und stürzen bei längeren Zeichenketten ab. Das ist so lange kein Problem, wie bei der bestimmungsgemäßen Nutzung nur kurze Eingaben auftauchen. Eventuell wird dieses Problem nie jemand bemerken. Hacker suchen aber gezielt nach solchen Fehlern und überschwemmen die Programme mit unsinnigen Eingaben.

Ein Beispiel für ein solches Problem (*Code Red*), das den Internet-Server von Windows-Systemen betrifft, werden Sie sehr häufig in den Log-Dateien Ihres Webservers finden. Dort tauchen Zeilen auf wie:

```
24.141.103.24 - - [09/Jun/2003:20:57:58 +0200] "GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%uc
bd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00
%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0" 400 330
```

Hier hat der aufrufende Rechner einen überlangen Parameter an das Programm `/default.ida` übergeben, das auf den Internet-Servern von Windows-Systemen vorhanden ist. Die ersten Zeichen dienen nur dazu, die von Microsoft vorgesehene Länge zu überschreiten. Die Zeichen dahinter sind ein Programmcode.

Viele Programme, wie hier der Webserver, laufen mit besonderen Rechten und übertragen diese Rechte beim Absturz auf Programmcode, der Teil der Eingabe ist.

Der hier als Beispiel angeführte Wurm *Code Red* ist nicht in der Lage, Apache-Webserver zu befallen, aber ein mit diesem Wurm befallener Rechner versucht nach einem Zufallsprinzip, andere Rechner zu befallen.

Weitere Informationen zum Wurm *Code Red* finden Sie im Cert Advisory unter `http://www.cert.org/advisories/CA-2001-19.html`

Auch in der Linux-Welt gibt es Programme mit ähnlichen Sicherheitsproblemen. In der letzten Zeit sind beispielsweise mehrfach Probleme bei FTP-Servern und SSH-Dämonen bekannt geworden. Sie können die Sicherheit bzw. Unsicherheit Ihrer Programme in der Regel nicht ohne weiteres abschätzen, sollten aber versuchen, sich über bekannte Probleme zu informieren.

Im Web bieten mehrere Webserver und Mailinglisten Sicherheits-Informationen für Linux. Linux-Systemverwalter sollten diese Informationen regelmäßig lesen und die zugehörigen Mailinglisten abonnieren.

2.8.1 OpenSUSE

Da Sie im vorliegenden Fall mit einem OpenSUSE-System arbeiten, ist deren Webserver die naheliegende Informationsquelle für Sicherheitsfragen. Der Vorteil dieser Website besteht darin, dass hier auch Lösungsvorschläge bzw. Aktualisierungen für Programme des OpenSUSE-Systems zu finden sind, auch wenn die eigentlichen Inhalte immer noch auf Novell-Servern liegen..

An der URL `http://forums.opensuse.org/tech-news/suse-security-announcements/` finden Sie aktuelle Sicherheitsinformationen.

Für Informationen per Mail finden Sie unter der Adresse `http://lists.opensuse.org/` eine Übersicht über Mailinglisten von OpenSUSE, die Sie von dieser Seite aus abonnieren können. Sicherheitsfragen behandeln vor allem die Listen `opensuse-securitiy-announce@opensuse.org` und `opensuse-securitiy@opensuse.org`. Über die Liste `security-announce` macht das Projekt selbst auf Probleme aufmerksam. In der Liste `security` können Sie auch Fragen stellen und sich an Diskussionen in englischer Sprache beteiligen.

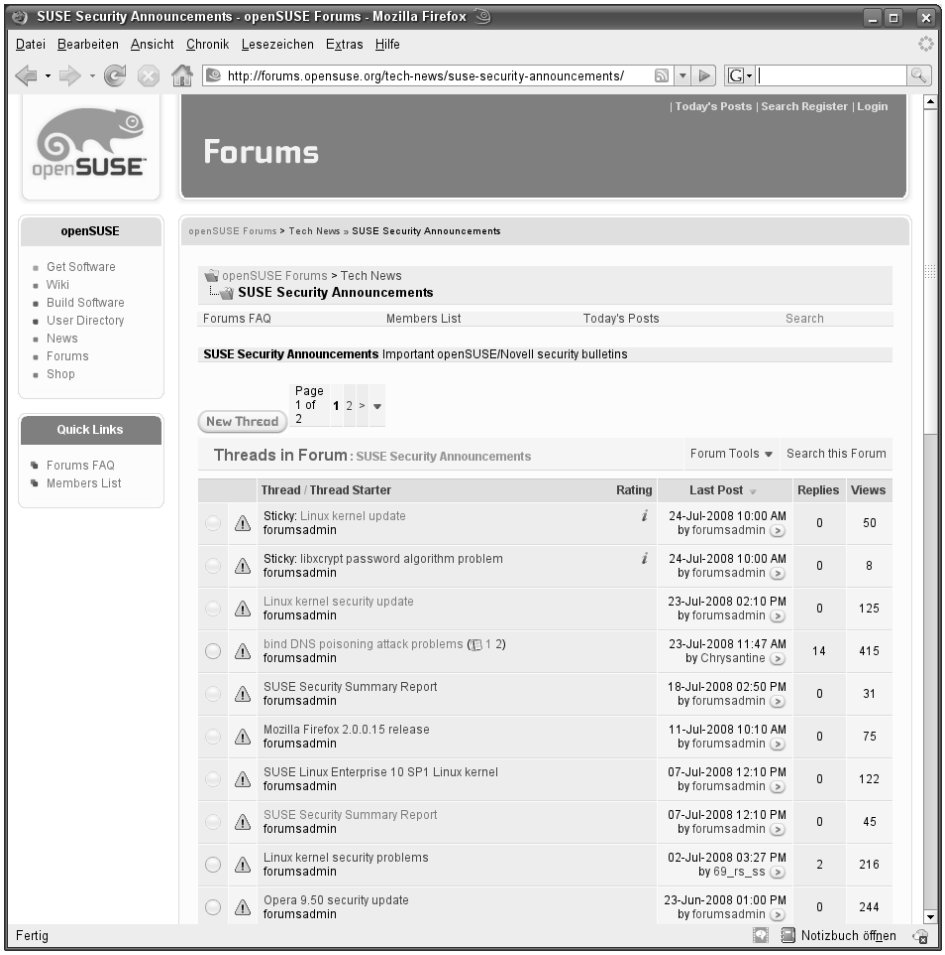

Abbildung 2.21: Sicherheitsinformationen bei openSUSE

2.8.2 Bugtraq/Securityfocus

Unter der Adresse `http://www.securityfocus.com/` finden Sie unabhängige Sicherheitsinformationen für verschiedene Betriebssysteme sowie Virusinformationen.

Abbildung 2.22: Sicherheitsinformationen bei SecurityFocus

Sehr weit verbreitet und beliebt ist die zugehörige Mailingliste `bugtraq@securityfocus.com`, die Sie an der URL `http://www.securityfocus.com/archive` abonnieren können. Wenn Sie Systeme mit verschiedenen Betriebssystemen betreuen, ist diese Liste eine wichtige Ergänzung zu der SUSE-Liste. Außerdem sind hier aktuelle Informationen oft deutlich schneller verfügbar.

2.8.3 Cert

Eine sehr anerkannte Institution in Sicherheitsfragen ist das CERT Coordination Center an der Carnegie Mellon University.

Eine Übersicht bekannter ausbeutbarer Programmfehler (Vulnerabilities) finden Sie ausgehend von der Seite `http://www.kb.cert.org/vuls/`.

Abbildung 2.23: Vulnerability Informationen beim Cert

Die dazugehörigen Lösungsvorschläge (Advisories) stehen an der URL `http://www.cert.org/advisories/`.

2.8.4 Heise Secutity

Relativ neu ist das Angebot des Heise-Verlags an den URLs `http://www.heisec.de` und `http://www.heise.de/security/`.

Die deutschsprachigen Heise-Seiten sind auf den hiesigen Markt abgestimmt. Sie finden hier aktuelle Sicherheitsmeldungen, eine Fülle von Hintergrundinformationen zum Thema Sicherheit und Diskussionsforen zum Thema. Unter der Rubrik *Dienste* können Sie Ihren Browser auf Sicherheitsmängel testen.

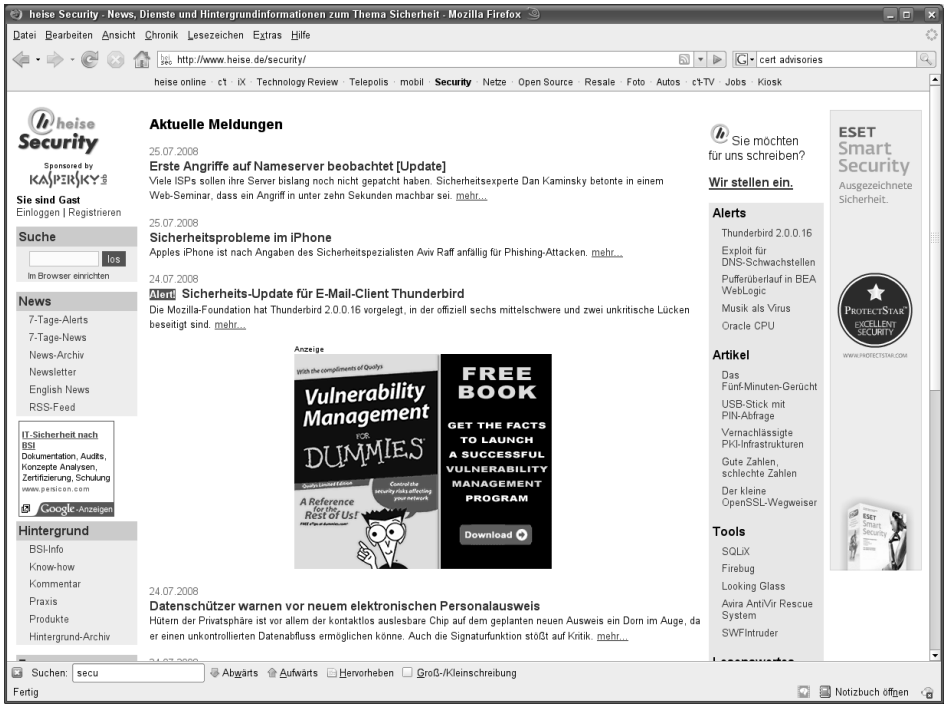

Abbildung 2.24: Heise Security

Wenn Sie Internet-Systeme mit guter Anbindung und vielen Nutzern betreiben, sollten Sie Stammgast auf diesen Seiten werden.

2.9 Programme und Systemdateien aktualisieren

Die Programme und Systemdateien, die Sie von den OpenSUSE-Datenträgern installieren, sind naturgemäß schon einige Wochen alt. In der Zwischenzeit wurden eventuell Fehler gefunden bzw. bereinigt. Der Vorteil der Linux-Gemeinde besteht ja gerade darin, dass sie Sicherheitsprobleme nicht verschweigt, sondern offen diskutiert und löst.

Sie können die verfügbaren Patches direkt vom FTP-Server unter der Adresse `http://download.opensuse.org/pub/opensuse/update/11.0/rpm/i586/` beziehen oder von einem der anderen FTP-Server mit den OpenSUSE-Dateien (siehe Kapitel 2.5). Einige der hier angebotenen `rpm`-Pakete kann man nicht zur Neuinstallation nutzen, da OpenSUSE in diese Pakete jeweils nur die korrigierten Dateien packt, um den Download-Umfang zu reduzieren. Erkennbar sind diese Dateien an der Endung `.delta.rpm`.

2.9.1 YOU

Einfacher als Laden vom FTP-Server ist OpenSUSEs automatisiertes Update-Verfahren, das *YaST Online Update* (YOU).

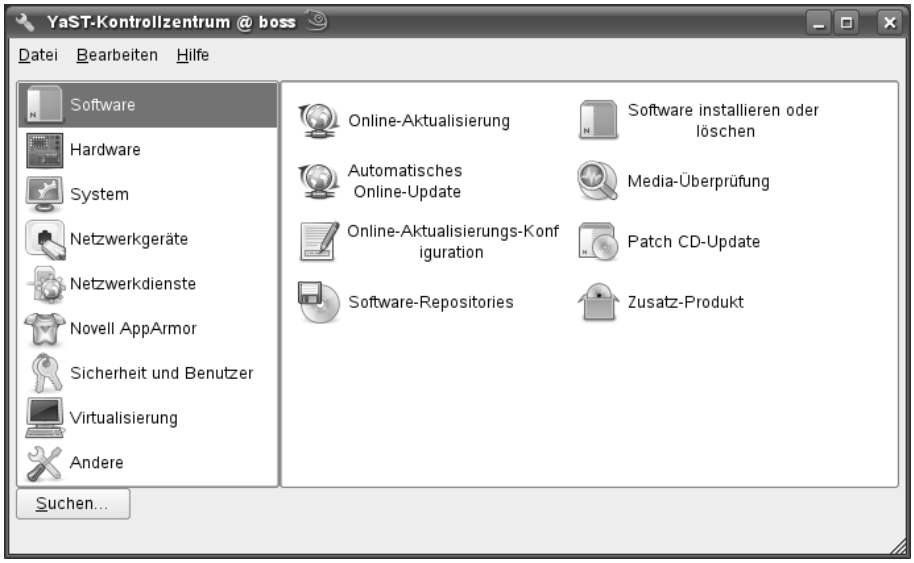

Abbildung 2.25: YaST: Online Aktualisierung

Wenn Sie YaST starten, finden Sie die Online-Aktualisierung in der Rubrik *Software*.

Hinweis: Das Online-Update kann natürlich nur mit einer funktionsfähige Internetanbindung klappen.

Bei der Installation bzw. beim ersten Start der Updatefunktion konfiguriert YaST diese aus dem Netz. Es sucht dazu einen Update-Server heraus, der gut erreichbar ist. Über die Online-Aktualiserungs-Konfiguration im Menü Software des YaST-Kontrollzentrums können Sie diesen Vorgang jederzeit neu auslösen.

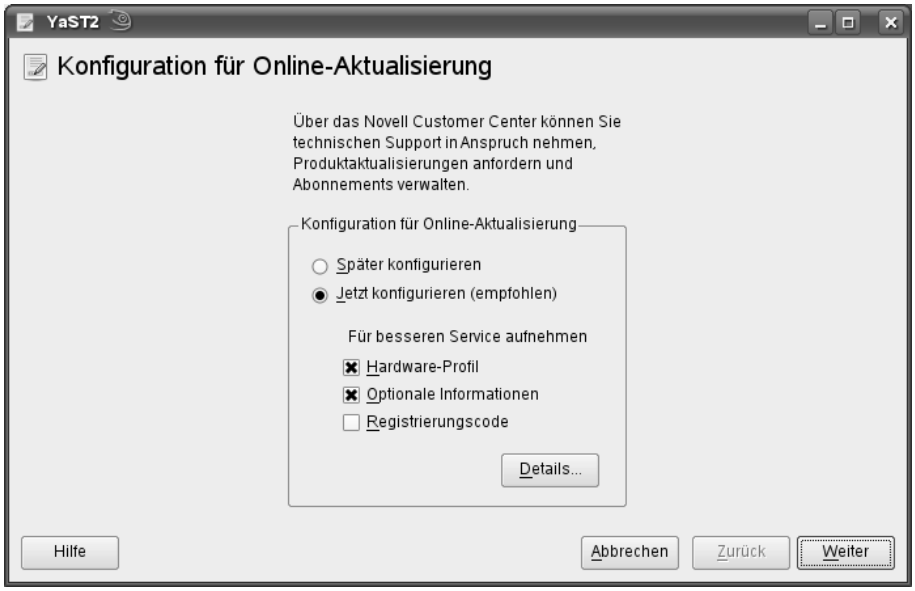

Abbildung 2.26: Konfiguration der Online-Aktualisierung

Mit dem Menüpunkt *Automatisches Online-Update* können Sie einen *Cronjob* einrichten lassen, der Ihr System automatisch jeden Tag aktualisiert, sofern er mit dem Internet verbunden ist.

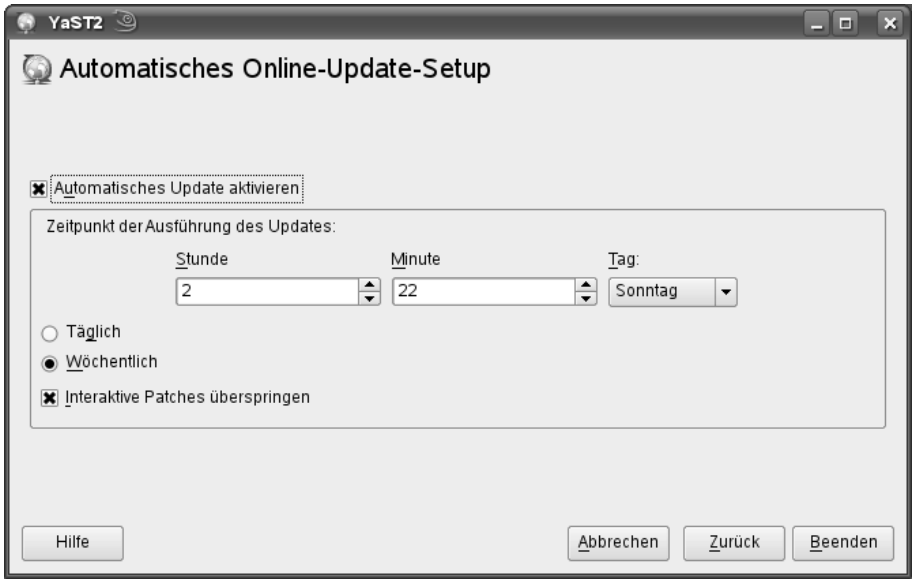

Abbildung 2.27: Online-Update: Automatisch

Sie sollten sich gut überlegen, ob Sie YaST so weit vertrauen, dass es Ihr System ohne Kontrolle aktualisieren darf. Das manuelle Update ist zwar etwas lästiger, aber Sie wissen dann auch genau, was YaST an Ihrem System verändert.

Beim normalen Online-Update lädt YaST eine Liste der zur Verfügung stehenden aktuelleren Pakete. Falls ein Update für das Online-Update zur Verfügung steht – auch das kann mal passieren – sehen Sie nur ein einziges Paket, welches Sie installieren müssen. Normalerweise bekommen Sie nach dem Laden der Dateiliste ein Auswahlfenster mit den verfügbaren Patches.

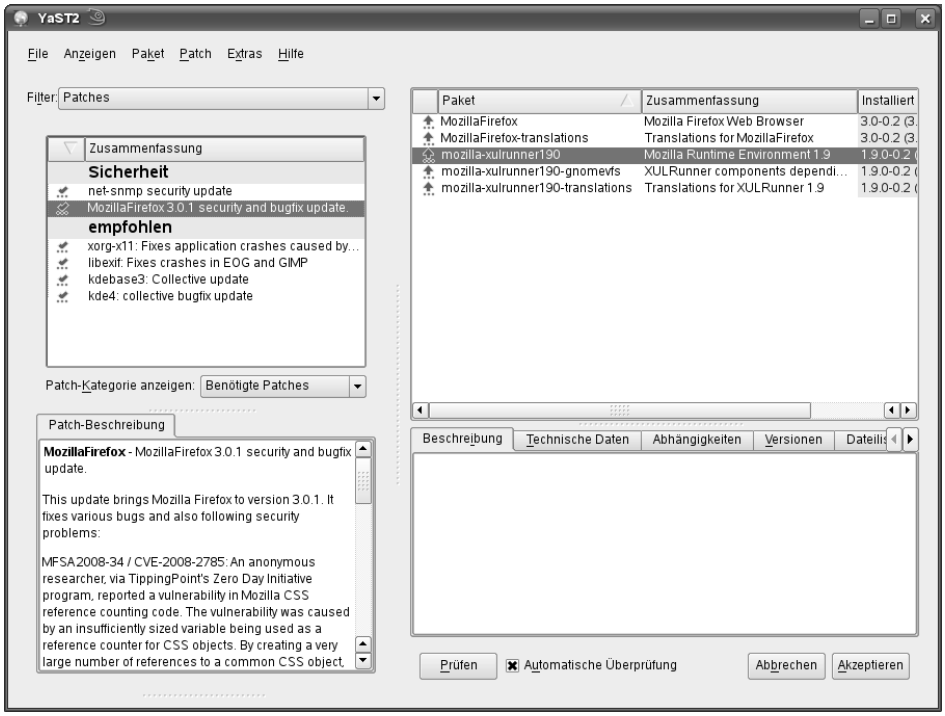

Abbildung 2.28: Online-Update: Liste der verfügbaren Patches

Bitte gehen Sie diese Liste durch. Mit einem Häkchen markiert YaST alle bei Ihnen installierten Pakete, die es aktualisieren möchte. Dabei sortiert es nach *sicherheitsrelevanten* Updates und *empfohlenen* Updates.

Wenn Sie dann auf *Weiter* klicken, beginnt YaST mit dem Laden der Pakete.

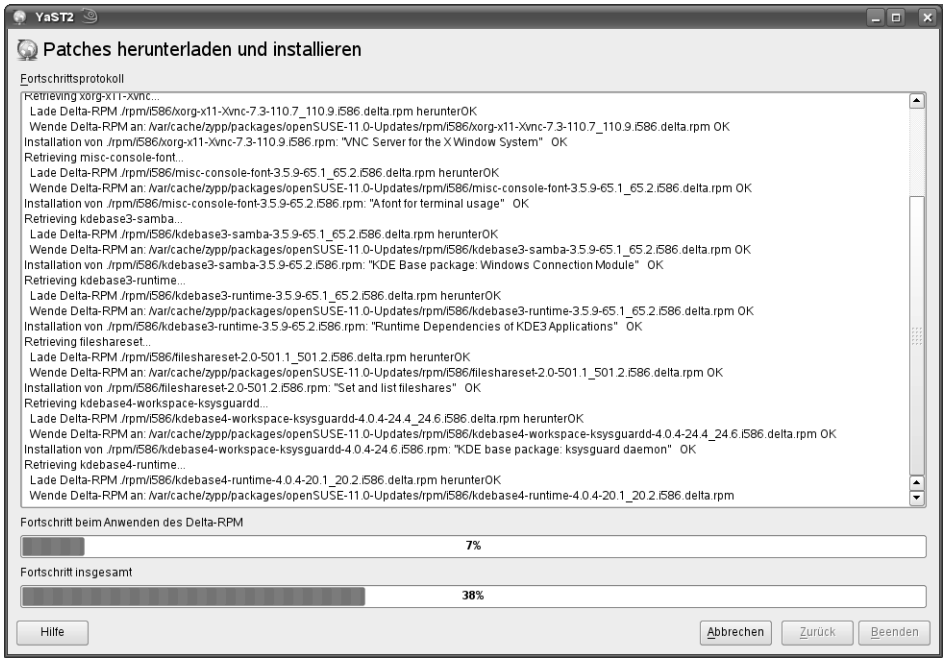

Abbildung 2.29: Online-Update: Laden der Patches

Nach dem Laden aller Pakete beginnt YaST, diese zu installieren und aktualisiert gegebenenfalls auch die Konfigurationsdateien.

Damit ist Ihr erstes Online-Update abgeschlossen.

Sie sollten das Updaten regelmäßig wiederholen, da OpenSUSE immer wieder neue Pakete zur Verfügung stellt. Die weiteren Updates gehen wesentlich schneller, da nur die in der Zwischenzeit erneuerten Pakete zu laden sind. Machen Sie das Update zu einer regelmäßigen Einrichtung!

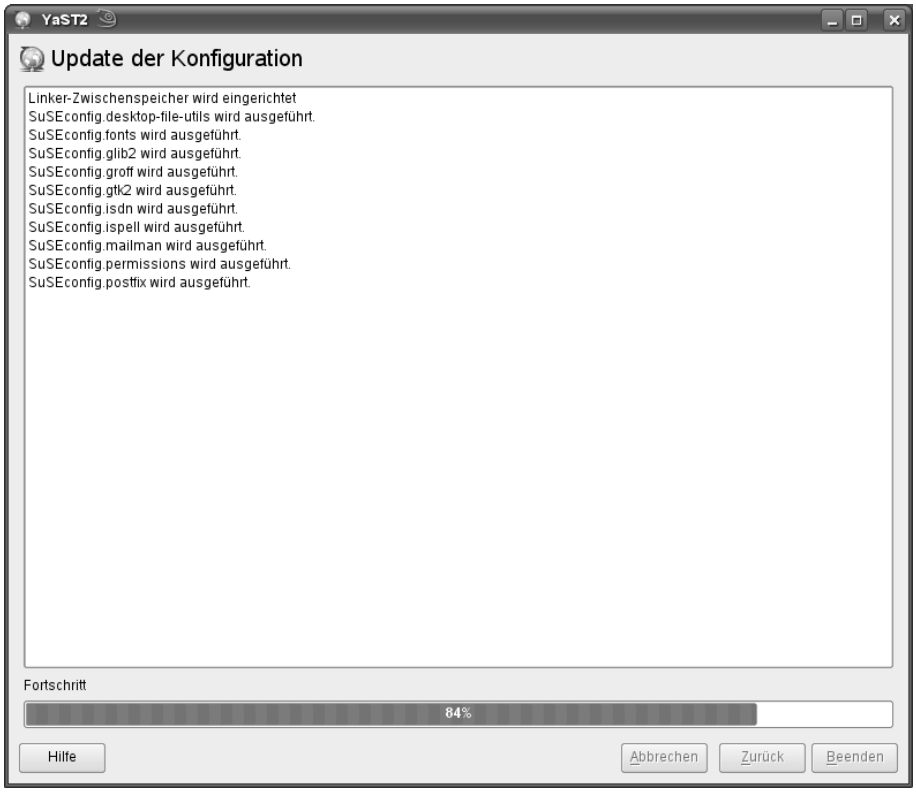

Abbildung 2.30: Online-Update: Aktualisierung der Konfigurationsdateien

2.10 Einbruchserkennung und Virenschutz

Das Aktualisieren von Programmpaketen dient dazu, Einbrüche und Schädigungen durch Viren zu erschweren, indem Sie Programme mit bekannten Sicherheitslücken durch korrigierte Versionen ersetzen.

2.10.1 Einbruchserkennung

Eine absolute Sicherheit vor Hackern kann aber auch dies nicht bieten. Wenn es zu Einbrüchen in den von Ihnen betreuten Systemen kommen sollte, sollten Sie diese möglichst schnell erkennen.

Einbrüche lassen sich nicht immer ganz einfach erkennen, da die Einbrecher mitunter Systemprogramme durch veränderte Versionen ersetzen. Beliebt sind Veränderungen an den Programmen `ps` und `ls`, damit diese die Verzeichnisse und Programme der Einbrecher nicht anzeigen.

Ein recht einfaches, aber wirkungsvolles System der Einbruchserkennung besteht daher darin, Prüfsummen der wichtigsten Systemdateien zu erstellen und diese regelmäßig zu vergleichen. Wenn Einbrecher Systemdateien verändern, ändern sich die Prüfsummen, was eindeutig auf einen Einbruch hinweist.

Die Autoren haben mit dem Programm *Claymore* zur Einbruchserkennung (Intrusion Detection), das Sie von `http://www.securityfocus.com/tools/1675` kostenlos laden können, gute Erfahrungen gemacht.

```
wget  http://www.securityfocus.com/data/tools/claymore03.tar.gz
```

Das Perl-Programmpaket ist sehr klein. Entpacken Sie das Archiv mit

```
tar  xvfz  claymore.tar.gz
```

Dabei entsteht ein Verzeichnis `claymore-0.3` (die Versionsnummer kann sich ändern), in das Sie mit

```
cd  claymore-0.3
```

wechseln.

Kopieren Sie das Programm in das Verzeichnis `/root/bin`

```
cp  claymore.pl  /root/bin
```

Das Programm arbeitet mit zwei Dateien:

- `light.list`
- `light.db`

Die erste Datei enthält eine Liste der zu überwachenden Programme mit vollständiger Pfadangabe, die zweite Datei zusätzlich die jeweiligen Prüfsummen. In diese Prüfsummen gehen sowohl der Dateiinhalt als auch das Dateidatum ein, so dass Veränderungen sofort zu erkennen sind.

Beide Dateien legt das Programm im Home-Verzeichnis des aufrufenden Benutzers ab, also in `/root/claymore-0.3`. Legen Sie also bitte dieses Verzeichnis an:

```
mkdir /root/claymore-0.3
```

Das Programm schlägt eine Liste der zu überwachenden Dateien vor, wenn Sie den Parameter `-m` mit angeben. Diese Liste können Sie so an die richtige Stelle bringen:

```
/root/bin/claymore.pl  -m  >  /root/claymore-0.3/light.list
```

Dann müssen Sie die Datei mit den Prüfsummen initialisieren:

```
/root/bin/claymore.pl  -r
```

Das dauert jetzt etwas, da sehr viele Dateien in der Liste stehen.

Jedes Mal, wenn Sie fortan

```
/root/bin/claymore.pl
```

aufrufen, erzeugt das Programm für jede Datei in der `light.list` eine Prüfsumme und vergleicht diese mit dem in der Datei `light.db` gespeicherten Wert.

Sowie es eine Abweichung gibt, gibt Claymore an die Konsole und die konfigurierbare Mailadresse eine Warnmeldung aus.

Einstellungen des Programms können Sie leicht verändern, vor allem den Mail-Empfänger für die Virenwarnungen.

```
claymore.pl (Auszug ab Zeile 21)
#########################################################################
# info to customize
$USER = '';  # (optional) address to email warnings, try
        ➥ 'root@localhost'
#########################################################################
# PATHs, these should be adjusted to match your system
$DB_FILE = "$ENV{'HOME'}/claymore-$::VERSION/light.db";
$LIST_FILE = "$ENV{'HOME'}/claymore-$::VERSION/light.list";
$MAIL = '/bin/mail';
```

Geben Sie in der Variablen `$USER` eine sinnvolle Mailadresse für die Warnungen an, möglichst eine auf einem anderen Rechner!

Um Einbrechern das Auffinden des Programms zu erschweren, sollten Sie die Dateinamen für die Listen und das Programm selbst ändern,

Wenn das Programm zu Ihrer Zufriedenheit konfiguriert ist, sollten Sie es per *Crontab* regelmäßig aufrufen lassen. Mit

```
05 * * * * /root/bin/claymore.pl
```

veranlassen Sie eine stündliche Überprüfung der Systemdateien.

Sie müssen nun aber bei jedem Online-Update daran denken, dass Sie die Datenbank von Claymore mit

```
/root/bin/claymore.pl  -r
```

neu erzeugen, da Sie sonst nach dem Update stündlich eine Fehlermeldung bekommen.

Hinweis: Auch das Programm Claymore und ähnliche Programme bieten keine absolute Sicherheit. Allein schon diese Beschreibung macht das System unsicherer, weil bekannter.

2.10.2 Virenschutz

Für Linux-Server gibt es Virenschutzprogramme zum Beispiel von H+B EDV, Sophos, McAfee, und FRISK Software International.

Zwar ist die Zahl der Linux-Viren gering, doch können Benutzer DOS/Windows-Viren in den freigegebenen Verzeichnissen ablegen. Da Viren sich leicht über allgemein freigegebene Verzeichnisse verbreiten können, sollten Sie diese Verzeichnisse regelmäßig auf Virenbefall untersuchen.

Ein auch unter Linux kommerzieller Virenscanner ist das Programm AntiVir der Firma H+B EDV. Für die private Nutzung ist das Programm jedoch kostenfrei. Nähere Informationen zu den Lizenzbedingungen und den Kosten dieser Software finden Sie unter der URL `http://www.antivir.de`.

Für die meisten Server dürfte die Nutzung von AntiVir kostenpflichtig sein. Glücklicherweise gibt es aber auch hier eine freie Software, das Programmpaket Clam AntiVirus.

Bei OpenSUSE finden Sie das Programm als Paket `clamav` in der Paketgruppe *Sicherheit*. Installieren Sie dieses Paket und die zugehörige Virus-Datenbank `clamav-db` unbedingt nach.

Hinweis: Die Programmversion von der Installations-DVD ist wegen des Publikations- Takts stets älter als die Version, die Sie direkt von den Seiten des Projekts laden können. Nur aktuelle Antivirenprogramme schützen. Aktualisieren Sie daher Clam AntiVirus möglichst gleich über den eingebauten Update-Mechanismus: `/usr/bin/freshclam`

Nach der Installation ist ClamAV sofort voll nutzbar.

Selbst wenn Sie das Programm nur auf Ihrem Server installieren, können Sie die Sicherheit für Ihr gesamtes Netzwerk erhöhen, indem Sie regelmäßig die Netzlaufwerke scannen.

Wenn die Anwender ihre Daten nur auf zentralen File-Servern speichern können, lassen sich Infektionen auf den Client-Rechnern zumeist sehr schnell bemerken.

Zum Testen können Sie mit dem Programm die Home-Verzeichnisse scannen:

```
/usr/bin/clamscan   -r /home
```

Mit dem Parameter `-r` (für rekursiv) legen Sie fest, dass ClamAV auch Unterverzeichnisse durchsuchen soll. Das Programm besitzt noch weitere nützliche Parameter:

Parameter	*Funktion*
`-h`	zeigt einen Hilfetext an
`--unzip`	wertet auch Dateien in ZIP-Archiven aus
`-v`	ausführlichere Meldungen
`--remove`	löscht infizierte Dateien
`--detect-pua`	Erkennt unerwünschte Anwendungen
`--recursive`	Auch Unterverzeichnisse testen

Tabelle 2.4: Einige Parameter von ClamAV

ClamAV ist einigermaßen schnell, wenn Sie nicht gerade die Parameter `--unzip` und `--recursive` angeben.

Zum Programmpaket ClamAV gehören die Dämon-Programme `freshclam` und `clamd`. Das Programm `freshclam` aktualisiert die Viren-Datenbnak in regelmäßigen Abständen und sollte daher unbedingt als Dienst über den `xinetd` starten.

Sofern Sie den Virenscanner häufiger nutzen, ist es sinnvoll, auch den `clamd` als Dienst zu starten. Der Virenscan erfolgt dann etwas schneller, da nicht jedes Mal die Datenbank neu eingelesen werden muss. Der Dämon wartet im Hintergrund auf Anfragen und muss nicht für jeden Auftrag neu gestartet werden.

Zum Automatisieren des Starts von ClamAV lesen Sie im Kapitel 4, »Vorgänge automatisch starten«.

Im Kapitel 14, »Linux als E-Mail-Server« lesen Sie, wie Sie Ihren Mailverkehr mit einem Virenscanner absichern.

2.11 USV

- Beim Planen Ihrer Server-Installation sollten Sie schon früh darüber nachdenken, wie Sie Ihre Systeme nicht nur gegen Softwarefehler, sondern auch gegen von Störungen wie Stromausfälle absichern.

Vor den Folgen eines Stromausfalls können Sie Server mit Anlagen zur *Unterbrechungsfreien Stromversorgung* (USV-Anlage) schützen. Derartige Geräte bekommen Sie für nahezu jeden Strombedarf. USV-Anlagen überbrücken einen Stromausfall für eine gewisse Zeit, die von der Batteriekapazität der Anlage abhängt. Sinkt der Ladezustand der Batterien der USV-Anlage unter einen kritischen Wert, so kann die Software den Rechner geordnet herunterfahren.

Für viele USV-Geräte finden Sie Linux-Software. Die Autoren haben bei den weit verbreiteten USV-Anlagen der Firma APC gute Erfahrungen mit der Software APCUPSD gemacht.

2.11.1 APCUPSD

Sie finden das Programmpaket `apcupsd` in der Paketgruppe System von OpenSUSE, zusätzlich finden Sie dort auch eine grafische Oberfläche im Paket `apcupsd-gui`.

Die aktuellste Version (derzeit 3.14.4) auch für OpenSUSE finden Sie an der Adresse `http://www.apcupsd.org/`.

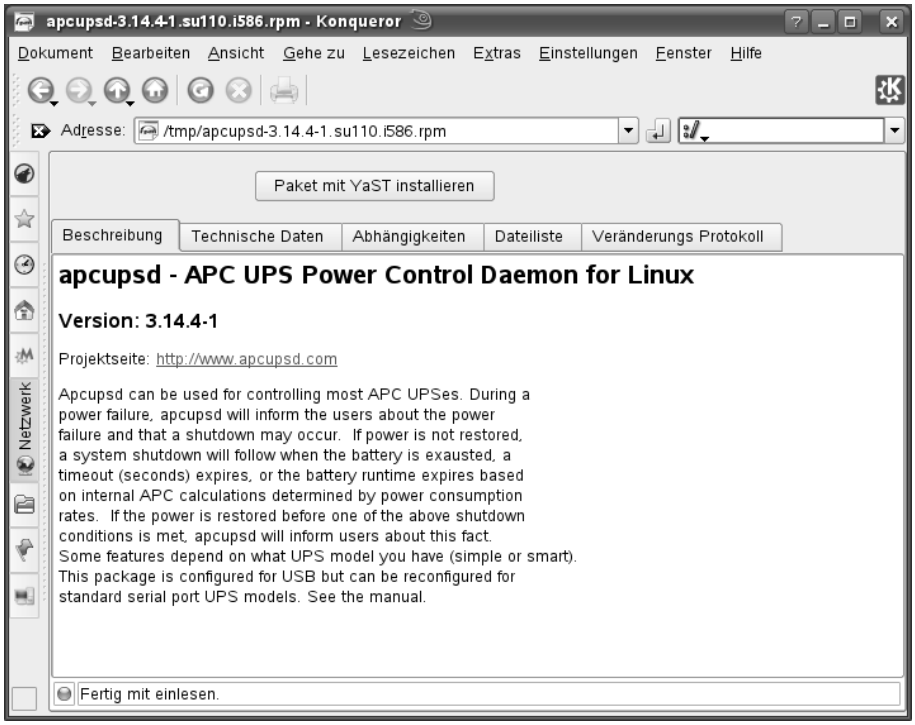

Abbildung 2.31: RPM-Datei mit YaST installieren

Nach der Installation müssen Sie die Konfigurationsdatei anpassen. Die wichtigsten Einstellungen finden Sie gleich am Anfang der gut dokumentierten Datei.

```
/etc/apcupsd/apcupsd.conf
## apcupsd.conf v1.1 ##
#
#  for apcupsd release 3.14.3 (20 January 2008) - suse
#
# "apcupsd" POSIX config file
```

```
#
# ========= General configuration parameters ============
#
# UPSNAME xxx
# Use this to give your UPS a name in log files and such. This
# is particulary useful if you have multiple UPSes. This does
# not set the EEPROM. It should be 8 characters or less.
#UPSNAME

# UPSCABLE <cable>
# Defines the type of cable connecting the UPS to your Computer
#
#   Possible generic choices for <cable> are:
#     simple, smart, ether, usb
#
#   Or a specific cable model number may be used:
#     940-0119A, 940-0127A, 940-0128A, 940-0020B,
#     940-0020C, 940-0023A, 940-0024B, 940-0024C,
#     940-1524C, 940-0024G, 940-0095A, 940-0095B,
#     940-0095C, M-04-02-2000
#
UPSCABLE smart

# To get apcupsd to work, in addition to defining the cable
# above, you must also define a UPSTYPE, which corresponds to
# the type of UPS you have (see the Description for more details).
# You must also specify a DEVICE, sometimes referred to as a port.
# For USB UPSes, please leave the DEVICE directive blank. For
# other UPS types, you must specify an appropriate port or address.
#
# UPSTYPE  DEVICE     Description
# apcsmart /dev/tty** Newer serial character device,
#                     appropriate for SmartUPS models using
#                     a serial cable (not USB).
#
# usb       <BLANK>   Most new UPSes are USB. A blank DEVICE
#                     setting enables autodetection, which is
#                     the best choice for most installations
#
# net  hostname:port  Network link to a master apcupsd
#                     through apcupsd's Network Information
#                     Server. This is used if you don't have
#                     a UPS directly connected to your
#                     computer
#
# snmp    hostname:port:vendor:community
```

```
#                       SNMP Network link to an SNMP-enabled
#                       UPS device. Vendor is the MIB used by
#                       the UPS device: can be "APC",
#                       "APC_NOTRAP" or "RFC" where APC is the
#                       powernet MIB,
#                       "APC_NOTRAP" is powernet with SNMP trap
#                       catching disabled, and RFC is the IETF's
#                       rfc1628 UPS-MIB. You usually want "APC".
#                       Port is usually 161. Community is
#                       usually  "private".
#
# dumb    /dev/tty**  Old serial character device for use
#                       with simple-signaling UPSes.
#
# pcnet    ipaddr:username:passphrase
#                       PowerChute Network Shutdown protocol
#                       which can be used as an alternative to SNMP
#                       with AP9617 family of smart slot cards.
#                       ipaddr is the IP address of the UPS mgmt
#                       card. username and passphrase are the
#                       credentials for which the card has been
#                       configured.
#
UPSTYPE apcsmart
DEVICE /dev/ttyS0
…
```

Den richtigen Wert für `UPSCABLE` finden Sie auch auf dem Kabel, das mit der USV geliefert wird. Weit verbreitet ist hier der Typ `940-0024B`.

Den `UPSTYPE` können Sie auf der Vorgabe `apcsmart` belassen. Die anderen Einstellungen dienen dazu, z. B. über ein Netzwerk auf die USV zuzugreifen.

Sehr wichtig ist die Wahl der richtigen Schnittstelle des Linux-Servers. Sie haben hier meist nur die Wahl zwischen `/dev/ttyS0` (erste serielle Schnittstelle) und `/dev/ttyS1` (zweite serielle Schnittstelle). Im Zweifelsfall probieren Sie die Einstellungen einfach aus. Die aktuellen Programmversionen unterstützen auch die Anbindung der USV-Anlage mittels USB.

Nun steht dem Start der Software nichts mehr im Wege.

```
/etc/init.d/apcupsd  start
```

startet das Programm.

Achten Sie einen Augenblick auf die Meldungen. Wenn das Programm keine Verbindung zur USV herstellen kann, meldet es nach kurzer Zeit seine Probleme wie folgt:

```
PANIC! Cannot communicate with UPS via serial port.
Please make sure the port specified on the DEVICE directive is
correct,
and that your cable specification on the UPSCABLE directive is
correct.
```

In diesem Fall haben Sie die falsche Schnittstelle oder den falschen Kabeltyp angegeben. Die Meldungen der USV können Sie auch jederzeit in der Datei `/var/log/apcupsd.events` nachlesen.

Wenn Sie die Funktion der USV und der Software testen wollen, müssen Sie sehr viel Geduld aufbringen. Ziehen Sie die Stromversorgung zur USV-Anlage ab. Das Gerät piept dann laut und meldet auf der Konsole einen Stromausfall. Wenn der Ladezustand der Batterien unter 5% gesunken ist, leitet die Software den *Shutdown* für den Rechner ein. Ganz zuletzt schaltet die Software auch die USV-Anlage ganz aus. Bei den Tests der Autoren hat es selbst bei einer kleinen USV mehr als eine halbe Stunde gedauert, bis die Batterien endgültig geleert waren. Wenn Sie besonders vorsichtig mit Ihrem Server umgehen wollen, schließen Sie zum Testen nur das serielle Kabel an die USV an, nicht die Stromversorgung des Servers. Hängen Sie dort dann lieber unkritische Verbraucher an, z. B. Monitore, Heizlüfter etc.

Wenn das Programm ohne Fehlermeldungen läuft, dann müssen Sie noch sicherstellen, dass die USV-Software auch automatisch startet. Dazu aktivieren Sie im YaST-Kontrollzentrum den `apcupsd` so, wie Sie bereits im Abschnitt 2.6 den `dhcpd` aktiviert haben.

2.11.2 Andere Programme

Die Firma APC bietet eine Linux-Version ihren Software *PowerChute* an. Sie können diese unter der URL `www.apcc.com/tools/download/` beziehen.

2.12 Datensicherung

Vor den Folgen von Hardware-Defekten, vor allem bei Festplatten, können Sie sich mit einem regelmäßigen Backup aller Daten schützen. Das vermeidet zwar nicht den technischen Defekt, ermöglicht aber, schadhafte Hardware ganz ohne oder nur mit geringen Datenverlusten zu ersetzen.

2.12.1 Backup auf DVD

Ein preiswertes Backup-Medium stellen DVDs dar. Wegen der niedrigen Preise der Rohlinge sichern immer mehr Anwender ihre Daten auf DVDs. Linux unterstützt

nahezu alle SCSI-Brenner und die meisten aktuellen ATAPI-Brenner.. Die benötigte Software CDRecord, Paket `cdrecord`, und XCDRoast, Paket `xcdroast`, liefert OpenSUSE mit. Die breite Unterstützung der modernen Blu-Ray-Medien ist inzwischen auch in Gang gekommen.

Anwender und Systemverwalter, die gern mit grafischen Oberflächen arbeiten, können zum Sichern auf CDs die Oberfläche K3B nutzen, welche die in der Standardinstallation bereits eingerichteten externen Anwendungen `cdrdao`, `cdrecord` und `mkisofs` voraussetzt.

Zum Sichern der Home-Laufwerke in mittleren und größeren Netzen sind die Kapazitäten von 4,7 GB bei DVDs leider meist zu klein. Daher nutzen viele Administratoren DAT-Streamer, die auf Magnetbändern immerhin 20 Gigabyte – oder auch mehr – sichern. Während man jedoch CDs und DVDs inzwischen auf fast jedem PC lesen kann, sind DAT-Streamer doch rarer.

2.12.2 Backup auf Bandlaufwerken

Eine gute Alternative zu CD/DVD Brennern sind DAT-Streamer, die eine Kapazität von 36 GByte pro Band besitzen. Da Streamer die Daten komprimieren können, sind effektive Kapazitäten bis zu 72 GByte möglich – viel mehr als selbst bei Double-Layer-DVDs.

Zum Steuern von Streamern gibt es inzwischen viele Linux-Programme, darunter auch professionelle Lösungen, in die man sich richtig einarbeiten muss. Sie können aber auch mit Linux-Bordmitteln wie `tar` bequem Daten auf DAT-Bänder sichern.

2.12.3 Professionelle Tools

Einige professionelle Tools zum Sichern mit Streamern sind zumindest bei bestimmten Nutzungsarten kostenlos. Zum Sichern auf zentralen Streamer-Servern besteht die Software aus einem Server- und einem Client-Programm.

Arkeia (http://www.arkeia.com)

Dieses kommerzielle Tool war lange Zeit für die Nutzung mit maximal zwei Linux-Clients kostenlos nutzbar. Es verfügt über eine grafische Oberfläche und eine sehr ausführliche Anleitung. Im Web sind viele Beschreibungen hierzu zu finden.

Amanda (http://www.amanda.org)

Der *Advanced Maryland Automatic Network Disk Archiver* ist ein Open-Source- Projekt, welches kaum Wünsche offen lässt. Die Anleitung im Amanda-Wiki ist inzwischen sehr umfangreich geworden..

2.12.4 Es geht auch mit tar & Co

Der Nachteil der professionellen Systeme besteht darin, dass sie sehr viel Vorbereitung benötigen. Sie müssen dazu einen Backup-Plan erstellen und die Bänder dazu passend vorbereiten und beschriften.

Wenn Sie ihre Sicherungen nicht so professionell und detailliert planen können oder möchten, können Sie auch mit den in allen Distributionen vorhanden Systemprogrammen arbeiten.

- `tar` (aus dem Paket `tar`) ist das Programm zum Lesen und Schreiben der Daten auf den Streamer.
- `mt` (aus dem Paket `cpio`) bzw. `mtst` (aus dem Paket `mt_st`) dient u. a. zum Spulen des Bandes.
- `buffer` (aus dem Paket buffer) puffert den Schreibstrom, so dass das Band gleichmäßig läuft.

Wenn die Pakete noch nicht installiert sind, sollten Sie dies zuerst nachholen.

Vorbereitungen

Vor dem Sichern müssen Sie das Gerät benennen, auf welches Sie schreiben möchten. Für den (ersten) DAT-Streamer gibt es normalerweise zwei Devices:

```
/dev/nst0
```

und

```
/dev/st0
```

`st0` ist ein Rewinding-Device, welches nach jedem Schreibvorgang das Band automatisch zurückspult. Wenn Sie mehrere Sicherungen hintereinander schreiben möchten, nehmen Sie besser das Non-Rewinding-Device `nst0`.

Wenn in Ihrem Server nur ein einziger DAT-Streamer eingebaut ist, können Sie einen Link

```
/dev/tape
```

anlegen, über den die Software den Streamer ohne weitere Device-Angabe findet:

```
ln -s /dev/nst0  /dev/tape
```

mt und mtst

Mit dem Kommando `mt` (das sich ableitet von *control magnetic tape drive operation*) kontrollieren Sie die Operationen eines Magnetbandes wie Spulen an den Anfang oder an bestimmte Stellen. Der normale Aufruf ist

```
mt  -f  <device>  <operation>
```

Falls Sie bereits einen passenden Link auf das Tape-Device eingetragen haben, können Sie die Device-Angabe weglassen und einfach schreiben:

```
mt <operation>
```

Wichtige Operationen sind:

Operation		*Bedeutung*
`Rewind`		Spult das Band an den Anfang zurück
`Tell`		Gibt die Position des Bandes aus
`Status`		Gibt Informationen über das Laufwerk und das Band
`seek <zahl>`		Steuert direkt die vorgegebene Blockposition an, das ist die Position, die auch `tell` ausgeben würde.
`fsf <zahl>`		Steuert direkt eine Dateiende-Markierung an, `fsf 1` die erste, `fsf 2` die zweite, ...
`Eof`		Springt zur letzten Dateiende-Markierung.

Tabelle 2.4: Parameter von mt

Anders als `mt` erkennt `mtst status` auch bei den moderneren DDS-Bändern die Bandart richtig.

buffer

Das Programm `buffer` puffert den Datenstrom zum Streamer bzw. vom Streamer, damit das Bandlaufwerk möglichst gleichmäßig arbeiten kann. Besonders nützlich ist `buffer`, wenn Sie auf einem übers Netz verbundenen Rechner speichern.

Die wichtigsten Parameter für `buffer` sind

- `-i` Device/Datei gibt an, woher `buffer` die Daten bekommt
- `-o` Device/Datei gibt an, wohin `buffer` die Daten schreiben soll (z. B. `/dev/tape`)

tar

Systemadministratoren kennen das Programm `tar` zum Packen bzw. Entpacken von Archivdateien. Sein ursprünglicher Zweck war das Archivieren auf Bandlaufwerken, daher auch der vollständige Name *Tape Archiver*.

Zum Erstellen (nicht komprimierter) Archive benutzt man `tar` üblicherweise in der Form

```
tar -cf  <Archivname>  <Quelle>
```

`tar` speichert aus Sicherheitsgründen nie absolute Pfade, also auch keine führenden Slashes im Dateinamen. Mit dem Parameter `-v` (Volume) können Sie zusätzlich ein

Label, einen Titel für das Archiv vergeben. Zum Auspacken dient der Befehl in der Form

```
tar -xf  <Archivname>
```

wobei es die Dateien dann in das aktuelle Verzeichnis schreibt.

Wenn Sie vergessen haben, ins richtige Zielverzeichnis zu wechseln, können Sie mit dem Parameter `-C <Zielverzeichnis>` ein anderes Zielverzeichnis angeben.

Mit

```
tar -tf  <Archivname>
```

können Sie sich das Inhaltsverzeichnis eines Archivs anschauen.

Sichern mit tar & Co

Ein einfacher Ablauf zur Sicherung des Home-Verzeichnisses könnte folgendermaßen aussehen:

```
mt rewind
```

spult das Band an den Anfang zurück

```
tar -cf /dev/tape /home -V "sicherung /home"
```

sichert das Home-Verzeichnis auf das Band (kann etwas dauern)

```
mt tell
```

gibt die aktuelle Blockposition am Ende der Sicherung aus.

Damit das Bandgerät gleichmäßiger arbeitet, können Sie den Datenstrom mit dem Programm `buffer` puffern:

```
mt rewind
```

spult das Band an den Anfang zurück

```
tar -cf - /home -V "sicherung /home" | buffer -o /dev/tape
```

sichert das Home-Verzeichnis auf das Band (gepuffert).

Das – Zeichen anstelle des Device-/Dateinamens bewirkt eine Ausgabe auf die Standardausgabe, die Sie dann zum Programm `buffer` umleiten.

Zum Zurückspielen der Sicherung dient die Befehlsfolge:

```
mt rewind
```

spult das Band an den Anfang zurück

```
cd /tmp
```

Zum Auspacken soll vorsichtshalber ein temporäres Verzeichnis dienen.

```
buffer -i /dev/tape | tar -xf -
```

spielt das Home-Verzeichnis vom Band ins Verzeichnis `/tmp`

Sollten sich mehrere Sicherungsdateien auf dem Band befinden, so müssen Sie jeweils mit `mt seek` oder `mt fsf` die entsprechende Startposition anfahren.

Sicherung auf einem anderen Rechner mit rsh

Über `rsh` (Remote Shell) kann man Befehle auch auf einem anderen Rechner ausführen. Aus Sicherheitsgründen ist dieser Zugriff in den Standardeinstellungen verboten.

Zuerst müssen Sie auf dem Rechner mit dem Bandlaufwerk den `rsh`-Server nachinstallieren, da OpenSUSE mit der Standardinstallation weder das Server- noch das Client-Paket einrichtet. Sie finden das Paket `rsh-server` in der Paketgruppe *Netzwerk*.

Nach der Installation müssen Sie den Dienst noch (wie im Abschnitt 2.7 für den POP-Dämon beschrieben) für den `xinetd` aktivieren. Sie finden den Dienst im Editor für den `xinetd` unter der Bezeichnung `shell`.

In der Datei `/etc/hosts.equiv` können Sie die Rechner- und Benutzernamen angeben, denen Sie einen Remote-Zugriff erlauben wollen. Tragen Sie hier den Rechner ein, von dem aus Sie arbeiten wollen und Ihren Benutzernamen.

```
/etc/hosts.equiv
#
# hosts.equiv   This file describes the names of the hosts which are
#               to be considered "equivalent", i.e. which are to be
#               trusted enough for allowing rsh(1) commands.
#
# hostname
192.168.1.10   ksparsam
```

Damit sollten Sie auf diesem Rechner Daten sichern können.

```
rsh  -l  ksparsam  boss  "mt rewind"
```

spult das Band an den Anfang zurück

```
tar -cf - /home -V "Sicherung /home" | rsh -l ksparsam boss "buffer -
o /dev/tape"
```

sichert das Home-Verzeichnis des lokalen Rechners auf das Band (gepuffert) des fernen Rechners.

```
rsh  -l  ksparsam  boss  "mt  tell"
```

gibt die aktuelle Blockposition aus, womit Sie jederzeit kontrollieren können, wieviel an Daten auf das Band gelangt ist.

Auch das Zurückspielen ist natürlich über das Netz möglich:

```
rsh -l ksparsam boss "mt rewind"
```

spult das Band an den Anfang zurück

```
rsh -l ksparsam boss "mt tell"
```

sollte als Ausgabe `At Block 0.` ergeben, woran Sie erkennen, dass das Zurückspulen erfolgreich war.

Mit

```
cd /tmp
```

wechseln Sie nun in ein Verzeichnis für temporäre Daten. In dieses Verzeichnis spielen Sie dann die Daten vom Band zurück mit

```
rsh -l ksparsam boss "buffer -i /dev/tape" | tar -xf -
```

anschließend können Sie von `/tmp` aus auf die benötigten Daten zugreifen.

Administratoren, die auf eine grafische Oberfläche verzichten können, sind also auch mit den normalen Linux-Bordmitteln gut bedient.